SHU DE ZHENGCHUXING

敏　泉

数的整除性

科学普及出版社

科　　目：11—63

统一书号：13051·1164

定　　价：　0.32 元

数的整除性

敏　泉

科学普及出版社

内 容 提 要

本书运用初等数论的一些基本概念和定理，讲述了怎样分析解答数论中一些有难度的问题。书中选取了大量的例题和习题，很多采自一些著名的数学竞赛试题，新颖而有代表性。全部习题都附有适当的提示和解答。对中学师生和数学爱好者，这是一本深浅适中的辅导读物。

数 的 整 除 性

敏 泉

责任编辑：吴之静

封面设计：窦桂芳

*

科学普及出版社出版（北京白石桥紫竹院公园内）

新华书店北京发行所发行　各地新华书店经售

中国科学院印刷厂印刷

*

开本：787×1092 毫米 1/32　印张：3 1/2　字数：78 千字

1981年10月第1版　1981年10月第1次印刷

印数：1－41,500 册　定价：0.32 元

统一书号：13051・1164　本社书号：0194

写在前面

下列诸数

$$\cdots,-3,-2,-1,0,1,2,3,\cdots$$

统称为整数。这种数虽然看起来很简单，但却有着极其有趣而深刻的性质。在数学中有一门叫做“整数论”(或“数论”)的分支专门研究它。这是一门历史悠久而至今还富有生命力的学科。早在公元前50年左右，在我国第一部数学名著《九章算术》的第一章中就开始讨论整数，介绍了辗转相除法；它与公元前三世纪欧几里得所著《几何原本》中介绍的辗转相除法是各自独立地总结出来的。五世纪时，在我国的《孙子算经》中更有闻名于世的中国剩余定理(即孙子定理)，也对整数做了研究。

由于整数比较具体，所以在学习现代数学时，它能提供朴素的背景。因此，对于爱好数学的青少年来说，能多了解一些整数的性质很有必要。此外，不少数论题目，其结论虽然十分明显，但论证却颇需技巧，因而也是培养、训练数学爱好者掌握逻辑推理与灵活思维的一个有效途径。这也许就是多年来在各国的数学竞赛中，初等数论的题目始终不衰的原因吧！

在这本小册子里，我们在中学数学的基础上，扼要地介绍了一些有关整数的简单的性质，并力图较系统地讲述数的整除性及其解题思路和方法。所选的习题有些是各国数学竞赛中的问题；我们还把某些性质和问题放在练习题中，读者如能动手做一做，必将大有收益。

目　　录

1. 初谈整除……………………………………………… 1
2. 奇与偶………………………………………………… 4
3. 再谈整除……………………………………………… 9
4. 公因数………………………………………………13
5. 三谈整除……………………………………………20
6. 组合数 C_n^k 与整除 ………………………………25
7. 素数…………………………………………………29
8. 整数的分解…………………………………………34
9. 整数的数码特征　整除性判别法…………………40
10. 完全平方数 ………………………………………47
11. 整数数列中的一些问题 …………………………53
12. 同余 ………………………………………………64
13. 剩余类及完全剩余组 ……………………………71
习题解答………………………………………………79

1. 初谈整除

读者在算术里早已知道两数相除的概念，以及除数和被除数的名称。所谓整除就是一个整数被另一个整数除尽，并且商也是整数。通常泛泛而说的整除性，其实还包含着两种涵义：一方面，研究两数作除法时的全面情况；另一方面，研究两数能否整除，以及探讨由此而引伸出来的有关问题。我们将会看到，这两方面是密切联系着的。

本书的内容，仅限于讨论整数的整除性问题。先从除法说起。

一个整数 b 除以整数 $a(>0)$，当然不一定恰好除尽，一般得一个商 q 和一个余数 r，亦即

$$b = aq + r。\tag{1}$$

按算术知识，可假设余数是非负的，且满足 $0 \leqslant r < a$。式(1)称为余数公式，对其运算过程也叫带余除法。

例如：-74 被 15 除，78 被 5 除，可分别写出

$$-74 = 15 \times (-5) + 1,\quad 78 = 5 \times 15 + 3。$$

定义 若整数 b 被整数 $a(>0)$ 除时，(1)式中余数 $r = 0$，即有整数 q，使得

$$b = aq,\tag{2}$$

就说 b 能被 a 整除，简记作 $a|b$。此时，也说 a 能整除 b，或 a 整除 b。同时，称 a 为 b 的因数，b 为 a 的倍数。

在本书中，如无特殊声明，$a, b, c, \cdots$ 等均表示整数。

性质1 若 $a|b$，$b|c$，那么 $a|c$。

证 由假设可知，有整数 m，n，使得 $b = am$，$c = bn$。

故 $c = bn = amn$, mn 仍是整数,即得 $a \mid c$。

性质 2 若 $a \mid b$, $a \mid c$, 那么对任何整数 k, l, 有

$$a \mid (kb + lc)。$$

证 由假设可知,有整数 m, n, 使得 $b = am$, $c = an$, 故 $kb + lc = k(am) + l(an) = a(km + ln)$, $km + ln$ 是整数,即得 $a \mid (kb + lc)$。

【例 1】 整数 b 被 $a (> 0)$ 除时,证明满足 $0 \leqslant r < a$ 的表示式(1)是唯一的。

证 设

$$b = aq + r, \ 0 \leqslant r < a,$$

如还有

$$b = aq' + r', \ 0 \leqslant r' < a。$$

将此两式相减得

$$0 = a(q - q') + r - r'。$$

由此 $a \mid (r - r')$, 但 $0 \leqslant |r - r'| < a$, 故得 $r - r' = 0$, 即 $r = r'$, 又 $a \neq 0$, $\therefore q = q'$。得证表示式(1)是唯一的。

【例 2】 设 a、b 都不是 3 的倍数,试证 $a + b$ 及 $a - b$ 有且仅有一个是 3 的倍数。

证 由假设可知, a 可写成 $3q_1 + 1$ 或 $3q_1 + 2$, 同样, b 可写成 $3q_2 + 1$ 或 $3q_2 + 2$, 这里的 q 都是整数。若 a、b 除以 3 后余数相同,那么 $a - b = 3(q_1 - q_2)$; 若余数不同,那么 $a + b = 3(q_1 + q_2 + 1)$。由 q 的整值性和余数的唯一性,证明所说的结论正确。

习 题 1

下列字母均表示整数:

1. 若 $a|b$，试证 $a|bc$。

2. 设 $a|b$，试证 $ak|bk$。

3. 设 $a|b$ 且 $c|d$，试证 $ac|bd$。

4. 若 $a+b+\cdots+d=g+h+\cdots+j$，$n$ 能整除 $b,c,\cdots,d,g,h,\cdots,j$，则 n 也能整除 a。

5. 若 $(m-p)|(mn+pq)$，那么 $(m-p)|(mq+np)$。

6. 对任两整数 a,b，试证 $a+b$、$a-b$、ab 三者之中至少有一个是3的倍数。

2. 奇 与 偶

奇数与偶数也是大家熟悉的概念。用整除的术语来说，能被 2 整除的整数 N 叫作偶数，不能被 2 整除的整数 N' 叫作奇数。由整除的定义可知，偶数 N 都可以表示成 $N=2n$ 形状，奇数 N' 都可以表示成 $N'=2n+1$ 形状。下列诸性质是明显的：

性质 3

奇数与奇数的和是偶数，奇数与奇数的积是奇数，

奇数与偶数的和是奇数，奇数与偶数的积是偶数，

偶数与偶数的和是偶数，偶数与偶数的积是偶数。

如果，偶数用“0”来表示，奇数用“1”来表示。那么性质 3 的结论就可以列成下表：

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

性质 4 在任意给定的三个整数 a、b、c 中必能从中选出两个，其和及差均为偶数。

证 把整数按奇数与偶数分成两类。a, b, c 三个数中至少有两个属于同一类(即同为奇数或同为偶数，请读者自证)，由性质 3 可知同属一类的两数之和是偶数，两数之差也是偶数。

从这两个简单的性质可以看出，我们实际上利用被 2 除的余数把全体整数划分成了两类，偶数能被 2 整除，即余数为 0，所以用 0 表示偶数类；奇数被 2 除时余数为 1，所以用 1 表

示奇数类。这种把全体整数进行划分成类的思想，乍看起来，平淡无奇，但是在解题时，若能对准问题的关键，有的放矢地加以灵活运用，却会得到奇妙的效果。

对于分类的思想，在第 12 节讲了同余之后，则可有更进一步的了解。

现在我们就如何运用上述基本性质，特别是分类思想，举一些例题。

【例 1】 相继两个自然数的乘积必是偶数。

解 设相继两个自然数为 $n, n+1$。易见两数中必有一为奇数，一为偶数，所以由性质 3 可知它们的乘积 $n(n+1)$ 是偶数。这也就是说，$2|n(n+1)$。

【例 2】 满足方程

$$x^2+y^2=z^2$$

的整数 x, y, z 中不能都是奇数。

证 用反证法。如若 x, y, z 都为奇数，那么由性质 3，可知 x^2, y^2, z^2 也都是奇数。又由性质 3 知 x^2+y^2 必是偶数，但 z^2 为奇数，故(3)式不真。由此矛盾，证得命题。

【例 3】 设 a_1, a_2, a_3 为任意给定的三个整数，把它们按任意顺序编排后记为 b_1, b_2, b_3。证明 $(a_1-b_1)(a_2-b_2)(a_3-b_3)$ 是偶数。

证 由于三个整数 a_1, a_2, a_3 中按奇、偶分类至少有两个属于同一类，不妨设 a_1, a_2 属同一类。而 b_1, b_2 是 a_1, a_2, a_3 中的两个，除去可能有一个为 a_3 外，其中至少有一个 b 与 a_1 或 a_2 属同一类(其实，这时就是 a_1 或 a_2)。这样，由性质 3 可知，或者 a_1-b_1 为偶数，或者 a_2-b_2 为偶数，不论哪一种情况，乘积 $(a_1-b_1)(a_2-b_2)(a_3-b_3)$ 总是偶数。

【例 4】 能否把平面上的凸 11 边形的每一顶点用 3 条对角线分别与另三个(不相邻的)顶点相连接？

证 用反证法来证明不可能作这样的连接。假若可以连接的话，设所用对角线的条数为 N。因每条对角线的两端有两个顶点，所以被 N 条对角线所连接着的顶点共出现 $2N$ 次。但另一方面，每一顶点恰要与另三个顶点相连接，即每一顶点恰好出现 3 次，共应出现 $3 \times 11 = 33$ 次，故有 $2N = 33$。此时右边为奇数 33，左边为偶数，矛盾。从而证得这样的连接法是不可能构作的。

其实，一般地可以证明：设 n，m 为奇数，平面上的凸 n 边形不能用对角线把每一顶点与另外 m 个顶点连接。

【例 5】 能否把 79 只电话用电线把 79 只中的每只恰与另外 19 只电话连接成直通电话。

证 用反证法来证明命题的结论是否定的。若不然，设连接所用电线的总条数为 n。因每条电线的两端连接着两只电话，所以被连接的电话共有 $2n$ 只。另一方面，由所设 79 只电话每只恰与另外 19 只相连接，所以相连接的总共应有 19×79 只。故得 $2n = 19 \times 79$。此时左边为偶数，右边为奇数，矛盾。这就证明了不能作这样的连接。

读者可以看出，例 5 和例 4 的本质是一样的。

【例 6】 证明任意改变某一自然数的各位数码的顺序后所得到的数，与原数之和不能等于 999。

证 原数应是三位数，记为 $\overline{abc}$。设此数改变顺序后记为 $\overline{a'b'c'}$，若它们的和 $\overline{abc} + \overline{a'b'c'} = 999$，那么必有

$$a + a' = 9,\ b + b' = 9,\ c + c' = 9。$$

但 a'，b'，c' 只不过是 a，b，c 的一个不同顺序的排列，所以 $a + b + c = a' + b' + c'$。故有

$$3 \times 9 = a + a' + b + b' + c + c' = 2(a + b + c)。$$

但此时左边为奇数，右边为偶数，矛盾。得证命题成立。

【例 7】 在 40 个人中每晚派出三人值班。证明排不出

这样的值班表，使得任两个人都同时值班一次且也只同时值班一次。试找出数 n，使每次派 n 人值班时，能排出这样的表。

证 考察某人参加的所有值班班次。若排得出所要求的值班表，那么在该人参加的全部班次中，其余 39 人每人都出现且仅出现一次。而这些班次中的每一班除去此人外，另二人是其余 39 人中的，这就是说，要把其余 39 人一个不漏地分成二人一班的若干班，由于 39 是奇数，显然这是办不到的。

当 $n = 2, 4, 14$ 时可排出这样的值班表。

习 题 2

1. 试用奇数与偶数的表示式证明性质 3。

2. 证明：在一段时间内，一群人相互握手，各人握手次数为奇数，则参加握手的人次必为偶数。

3. 试说明三个整数 a、b、c 中至少有两个同为奇数或同为偶数。

4. 设 a 为奇数，$a \geq 3$，试证 $8|(a^2 - 1)$。

5. 试证 $a - 1$ 与 $a^3 - 1$ 的奇偶性相同。 $a \pm b$ 与 $a^3 \pm b^3$ 的奇偶性相同。

6. 试把例 3 推广到一般情形，并证明之。

7. 试把例 5 推广到一般情形，并证明之。

8. 设 29 个省、市的乒乓球队参加友谊邀请赛，能否安排出这样的比赛场次，使每个队恰好参加奇数次比赛？

9. 设有 1979 位代表参加的一个大型学术会议，在会议中组织了许多小型讨论会，若每次讨论会参加的人数都是偶数个，能否作出这样的安排，使每个代表恰好参加奇数次小型讨论会？

10. 证明在空间中不存在这样的凸多面体，它有奇数个面，每个面又都是奇数边形。

11. 设 $f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n$ 是整系数多项式，若 $f(0)$，$f(1)$ 都是奇数，那么 $f(x)=0$ 无整数根。

3. 再 谈 整 除

本节，我们将用实例进一步介绍解整除问题的一些基本方法。这里只涉及读者熟悉的二项定理，因式分解，余数公式及数学归纳法等最简单的数学工具。其中常用的公式有

$$(a+b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + \cdots + \frac{n(n-1)\cdots(n-k+1)}{k!}a^{n-k}b^k + \cdots + b^n; \quad (1)$$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}); \quad (2)$$

当 n 为奇数时，

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots + b^{n-1})。 \quad (3)$$

【例 1】 若 $5|(a+b)$，则 $25|(a^5+b^5)$。

证 注意到二项展开式，有

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 = a^5 + b^5 + 5ab(a^3+b^3) + 10a^2b^2(a+b)。$$

由于已知 $5|(a+b)$，又 a^3+b^3 有因式 $a+b$，所以，25 能整除 $(a+b)^5$，$5ab(a^3+b^3)$ 及 $10a^2b^2(a+b)$。因此按习题 1 第 4 题可知：25 能整除 a^5+b^5。

【例 2】 试证：和数 $222^{555}+333^{444}$ 能被 7 整除。

证 由余数公式，有

$$222 = 7 \times 31 + 5, \quad 333 = 7 \times 47 + 4$$

由二项公式(1)可得

$$222^{555} + 333^{444} = (7 \times 31 + 5)^{555} + (7 \times 47 + 4)^{444}$$

$$= 7N + 5^{555} + 4^{444},$$

其中N是某整数。又由(3)可得

$$5^{555} + 4^{444} = (5^5)^{111} + (4^4)^{111} = (5^5 + 4^4)M,$$

其中M是某整数。而

$$5^5 + 4^4 = 3381 = 7 \times 483。$$

故按性质1得证

$$7 | (222^{555} + 333^{444})。$$

【例3】 试证：对任何正整数n，$3 \times 5^{2n+1} + 2^{3n+1}$能被17整除。

证 利用公式(2)，

$$3 \times 5^{2n+1} + 2^{3n+1} = 15 \times 5^{2n} + 2 \times 5^{2n} - 2 \times 5^{2n} + 2^{3n+1}$$
$$= 17 \times 5^{2n} - 2(5^{2n} - 2^{3n})$$
$$= 17 \times 5^{2n} - 2(25^n - 8^n)$$
$$= 17 \times 5^{2n} - 2(25 - 8)(25^{n-1} + \cdots + 8^{n-1})$$
$$= 17[5^{2n} - 2(25^{n-1} + \cdots + 8^{n-1})]。$$

证毕。

【例4】 试证：$N = 42^n [2^n(42^n - 1) - 1] + 1$能被3403整除，其中$n$是正整数。

证 注意到$3403 = 41 \times 83$，依公式(2)，

$$N = (42 \times 2)^n(42^n - 1) - (42^n - 1)$$
$$= (42^n - 1)(84^n - 1)$$
$$= (42 - 1)M_1 \times (84 - 1)M_2$$
$$= 3403M_1M_2,$$

其中M_1, M_2均为正整数。命题证毕。

【例5】 试证：和数$2222^{5555} + 5555^{2222}$能被7整除。

证 注意到

$$2222 = 7 \times 317 + 3, \quad 5555 = 7 \times 793 + 4$$

和公式(1)、(2)，有

$$2222^{5555}+4^{5555}=(2222+4)M=7\times318M,$$
$$5555^{2222}-4^{2222}=(5555-4)N=7\times793N。$$

所以

$$2222^{5555}+5555^{2222}=(2222^{5555}+4^{5555})+(5555^{2222}-4^{2222})-(4^{5555}-4^{2222})=7\times(318M+793N)-4^{2222}\times(4^{3333}-1)$$

而

$$4^{2222}(4^{3333}-1)=4^{2222}[(4^3)^{1111}-1]=(4^3-1)L=7\times9L$$

代入得：

$$2222^{5555}+5555^{2222}=7\times(318M+793N-9L)$$

得证命题成立。

从上面五个例子可以看出，解这种类型的问题，所用到的数学工具不多，但要求对基本公式能运用自如，特别要学会如在例3、例5演算中，先加一项 2×5^{2n}，4^{2222} 等，接着就减该项等技巧，这些都是解题时常用的手法。

【例6】 试证对任何正整数 n，$A_n=5^n+2\times3^{n-1}+1$ 能被8整除。

证 用数学归纳法。当 $n=1$ 时，$A_1=5+2+1$，命题成立。假设当 $n=k$ 时命题成立。当 $n=k+1$ 时，

$$A_{k+1}=5^{k+1}+2\times3^k+1=5\times5^k+6\times3^{k-1}+1$$
$$=5(5^k+2\times3^{k-1}+1)-4(3^{k-1}+1)。$$

由于 3^{k-1} 为奇数，故 $3^{k-1}+1$ 为偶数，所以 $4(3^{k-1}+1)$ 是8的倍数，结合归纳假设知上式右边能被8整除，即 $8|A_{k+1}$，证得命题对任何自然数 n 成立。

需要指出的是，有许多能用二项定理或因式分解的整除问题，常可用数学归纳法来给出证明，如这里的例子就是。

习 题 3

1. 设两数 x、y 之和为 7 的倍数，试证：$49 \mid x^7 + y^7$。

2. 试证：$N = 2^{10} - 2^8 + 2^6 - 2^4 + 2^2 - 1$ 能被 9 整除。

3. 试证：$6^{2n} - 1$ 能被 35 整除，其中 n 为正整数。

4. 试证：$1978^{1978} + 1980^{1979} - 1981$ 能被 1979 整除。

5. 设 n 为正偶数，那么 $13^n + 6$ 能被 7 整除。

6. 设 p、n 为自然数，证明 $p^n + (p-1)(p-2)n - 1$ 能被 $(p-1)^2$ 整除。

7. 证明：多项式 $a^{n+1} - (a-1)n - a$ 能被 $(a-1)^2$ 整除，其中 n 为自然数。

8. 试用数学归纳法证例 3 中的命题。

9. 设 n 为自然数，试证：

(i) $6^{2n} + 3^{n+2} + 3^n$ 能被 11 整除；

(ii) 设 l 为固定的正整数，若 $d \mid (a+b+c)$，$d \mid (a^l - b^l)$ 且 $d \mid (b^l - 1)$，那么对任何自然数 n，$d \mid (a^{ln+1} + b^{ln+1} + c)$。（提示：对 n 用数学归纳法。注意例7是它的一个特殊情况，试由此题再给出几个具体的数值例子）。

4. 公 因 数

在小学算术里，曾学习过整数的因数、公因数、最大公因数和倍数、公倍数、最小公倍数的意义。整数中许多较为深刻的性质，都要以这些最基本的概念作基础，在解整除问题的过程中也离不开它们。为此，在这两节中，我们还是从原始概念出发，从头谈起。

定义 若正整数 c 能整除正整数 a 及 b，就称 c 是 a 和 b 的一个公因数。a、b 的诸公因数中最大的一个，设为 d，叫作 a 和 b 的最大公因数，记作 $(a,b)=d$。

如 12、18 两数有公因数 1、2、3、6，其中最大者为 6，所以 6 是 12 和 18 的最大公因数，即 $(12,18)=6$。

易见，可将此定义推广到几个数的最大公因数。

性质 5 若 $a=bq+c$，则 $(a,b)=(b,c)$。

证 设 k 是 a、b 的公因数，由习题 1 第 4 题知 k 也能整除 c，所以 k 也是 b、c 的公因数。反之，设 k' 是 b、c 的公因数，显然，k' 也是 a 的因数，所以 k' 又是 a、b 的公因数。这就是说，a、b 的所有公因数就是 b、c 的所有公因数，从而两者的最大公因数是同一个数。得证 $(a,b)=(b,c)$。

系 若 $b|a$，那么 $(a,b)=b$。

求两个正整数的最大公因数常用的方法是辗转相除法。早在公元前 50 年左右，我国第一部数学名著——《九章算术》第一章（方田章）的约分术中就已指出："置分母、子之数，以多减少，更相减损，以求其等也，以等数约之。"这与欧几里得（Euclid，公元前三世纪希腊人）著的《几何原本》第七卷第二

题求最大公因数的辗转相除法相一致。具体地讲，例如求1218 和 546 的最大公因数，用辗转相除法计算的格式如下：

2	1218	546	4
	1092	504	
3	126	42	
	126		

即先用较小的一个数 546 作为除数，去除 1218，得余数 126；然后以 126 为除数，去除上一次的除数 546，得余数 42；再以 42 为除数，去除上一次的除数 126，此时刚好除尽，那么这最后一个除数 42（也就是最后一个不为零的余数）便是 1218 和 546 的最大公因数。一般地，我们可写出：

性质 6 用辗转相除法求 a、b 的最大公因数，就是以每次的余数为除数去除上一次的除数，直至余数为 0，那么最后一次的除数（亦即最后一个不为零的余数）便是 a 和 b 的最大公因数。

证 我们把辗转相除法的计算过程用带余除法的公式表示出来，逐次的除法可写成

$$
\begin{aligned}
&b = aq_1 + r_1,\\
&a = r_1q_2 + r_2,\\
&r_1 = r_2q_3 + r_3,\\
&\cdots,\\
&r_{n-2} = r_{n-1}q_n + r_n,\\
&r_{n-1} = r_nq_{n+1}。
\end{aligned}
\qquad (1)
$$

由上述诸式，按性质 5 我们有

$$(b,a) = (a,r_1) = (r_1,r_2) = \cdots = (r_{n-1},r_n) = r_n。$$

性质 7 若 $(a,b) = d$，那么存在着整数 k、l，使得 $ak + bl = d$。

证 由性质6知 $d = r_n$。现用归纳法证明，当
时，因有

$$r_1 = b - aq_1,$$

以及

$$r_2 = a - r_1q_2 = a - (b - aq_1)q_2 = a(1 - q_1q_2) - bq_2,$$

显见命题对 $n = 1, 2$ 成立。假设命题对 r_{n-1} 及 r_{n-2} 分别有整数 k'', l'' 及 k', l' 使 $r_{n-2} = ak'' + bl''$，$r_{n-1} = ak' + bl'$。则

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_n \\ &= ak'' + bl'' - (ak' + bl')q_n \\ &= a(k'' - k'q_n) + b(l'' - l'q_n), \end{aligned}$$

即证得命题对一切 n 成立。证毕。

定义 若 a 和 b 的最大公因数是1，即 $(a,b) = 1$，则称 a 与 b 是互素的。

下面的定理是互素的判定定理和有关性质。

系 a、b 互素即 $(a, b) = 1$ 的充分必要条件是存在着整数 s 和 t，使 $as + bt = 1$。

证 必要性是性质7的直接推论。现设有 s, t 使 $as + bt = 1$，而 d 是 a 与 b 的最大公因数，则 $d|a$，$d|b$，于是 $d|(a,b)$，即 $d|1$，从而 $d = 1$。

性质8 若 $(a,b) = 1$，则 $(a, bc) = (a, c)$。

证 设 d 是 a、c 的公因数。由性质1，d 也是 bc 的因数，所以 d 也是 bc、a 的公因数。

倒过来，设 d' 是 bc 与 a 的公因数。因 $(a, b) = 1$，故由性质7的系，存在着整数 k, l，使 $ak + bl = 1$，所以有 $ack + bcl = c$，因此，d' 也能整除 c，即 d' 也是 a、c 的公因数。这就证明了，bc、a 的所有公因数就是 a、c 的所有公因数，从而它们的最大公因数相同。证毕。

现在我们举几个例子：

【例1】 如 $(a,b)=1$，那么

$$(a,a+b)=(a+b,2a+b)=(3a+2b,2a+b)=1。$$

证 由于

$$a+b=a\cdot 1+b,$$

按性质5得

$$(a+b,a)=(a,b)=1。$$

同理，易得另外两个最大公因数也等于1。

【例2】 设 n 是正整数，试证：$n+(n+1)$ 与 $n^2+(n+1)^2$ 互素。

证 由于

$$-(2n+1)[n+(n+1)]+2[n^2+(n+1)^2]=1,$$

故由性质7的系，即证得

$$(n+(n+1),n^2+(n+1)^2)=1。$$

【例3】 证明 2^p-1 和 2^q-1 互素的充要条件是 p 和 q 是互素的。

证 必要性。假如 $(p,q)=a>1$，记 $p=ap_1$，$q=aq_1$ 的话，那么 $2^{ap_1}-1$ 和 $2^{aq_1}-1$ 两者都能被 2^a-1 整除，因 $a>1$ 故 $2^a-1>1$。即 2^p-1 与 2^q-1 不互素。这个矛盾说明条件是必要的。

充分性。若 $(p,q)=1$，不妨设 $p>q$，由辗转相除法和性质5，

$$p=ql_1+r_1,\quad q=r_1l_1+r_2,\quad \cdots,\quad r_{n-2}=r_{n-1}l_n+r_n,$$
$$r_{n-1}=r_nl_{n+1},$$
$$1=(p,q)=(q,r_1)=(r_1,r_2)=\cdots=(r_{n-1},r_n)=r_n。$$

若 $(2^p-1,2^q-1)=d$，那么，由于

$$2^p-1=2^{ql_1+r_1}-1=2^{r_1}(2^{ql_1}-1)+(2^{r_1}-1)$$
$$=(2^q-1)N+(2^{r_1}-1),$$

其中 N 是整数，依性质5，有 $(2^q-1,2^{r_1}-1)=d$。

依此方法继续讨论，可得

$$\begin{aligned}d &= (2^p-1,2^q-1)=(2^q-1,2^{r_1}-1)\\&=(2^{r_1}-1,2^{r_2}-1)=\cdots\\&=(2^{r_{n-1}}-1,2^{r_n}-1),\end{aligned}$$

注意到 $r_n=1$，即得 $d=1$。故条件是充分的。证毕。

注 如在证命题："若 A 则 B"遇到困难时，在某些场合，可证其等价的逆否命题："非 B 推出非 A"。上例的必要性证明，就采用了这样的方式。

【例 4】 若在正整数 $a_1,a_2,\cdots,a_n$ 与 $b_1,b_2,\cdots,b_m$ 中各任取一数 a_i 与 b_j 都有 $(a_i,b_j)=1$，那么

$$(a_1a_2\cdots a_n,b_1b_2\cdots b_m)=1。$$

证 利用性质 8，因 $(a_i,b_2)=1$，故 $(a_i,b_1b_2)=(a_i,b_1)=1$。对于 b 的各数用归纳法易证，对任一 a_i，$(a_i,b_1b_2\cdots b_m)=1$ 成立。然后再由性质 8 及刚刚证得的式子，可知

$$(a_1a_2,b_1b_2\cdots b_m)=(a_1,b_1b_2\cdots b_m)=1,$$

对 a 的各数用归纳法就证得 $(a_1a_2\cdots a_n,b_1b_2\cdots b_m)=1$。

特别当 $(a,b)=1$，n、m 为任意正整数时，$(a^n,b^m)=1$。

【例 5】 试证 $\log_2 3$ 是无理数。

证 用反证法。若 $\log_2 3=p/q$，p，q 是正整数，且 $(p,q)=1$。由对数的定义可知，$2^{p/q}=3$，即 $2^p=3^q$。因 $(2,3)=1$，由例 4 知 $(2^p,3^q)=1$。这样，等式 $2^p=3^q$ 不能成立，矛盾。得证 $\log_2 3$ 是无理数。

一般地，设 a，b 为大于 1 的自然数，且 $(a,b)=1$，那么 $\log_a b$ 是无理数。其证明方法与例 5 类同。

【例 6】 设 n 是自然数，试证下列诸数是两两互素的：

$$2^2+1,\ 2^{2^2}+1,\ \cdots,\ 2^{2^n}+1。$$

证 记 $a_k=2^{2^k}$，$k=1,2,\cdots,n$。因为

$$a_{k+1}-1=2^{2^{k+1}}-1=(2^{2^k})^2-1=a_k^2-1$$

$$=(a_k-1)(a_k+1),$$

所以数列$\{a_k-1\}$的每一项能被它前面的各项整除，且由于$(a_k+1)|(a_{k+1}-1)$，故当$l<m(1\leqslant l<m\leqslant n)$时，有$(a_l+1)|(a_m-1)$，因此，

$$\begin{aligned}2^{2^m}+1&=a_m+1=a_m-1+2\\&=q(a_l+1)+2\\&=q(2^{2^l}+1)+2。\end{aligned}$$

这样，奇数$2^{2^m}+1$和$2^{2^l}+1$的最大公因数d(当然是奇数)也是2的因数，故得$d=1$。证毕。

习 题 4

1. 求10231和1820的最大公因数。

2. 设c是a、b的公因数，试证$c|(a, b)$。

3. 三个正整数a_1，a_2，a_3的最大公因数是指该三数的公因数中最大的一个，记为(a_1,a_2,a_3)。试证：

$$(a_1,a_2,a_3)=((a_1,a_2),a_3)。$$

4. 若$a=cq+r$，$b=cq_1+r_1$，试证：

$$(a,b,c)=(r,r_1,c)。$$

5. 试证$(am, bm)=(a, b)m$。由此，若$(a, b)=d$，$a=a_1d$，$b=b_1d$，则$(a_1,b_1)=1$。

6. 设正整数$a>1$，$b>1$且$(a,b)=1$，那么必存在着正整数ξ，η使$a\xi-b\eta=1$，其中$0<\xi<b$，$0<\eta<a$。

7. 已知$(a, b)=1$的充要条件是存在整数k，l使得$ak+bl=1$(性质7的系)。试问：$ak+bl=d$是否为$(a, b)=d$的充要条件?

8. 设ax_0+by_0是形如$ax+by$(x、y是任意整数，a、b

是正整数)的数中最小的正数，那么 $(a,b)=ax_0+by_0$。

9. 若 $(a,b)=1$，那么 $(a+b,a^2+b^2)=1$ 或 2。

10. 试证：$\sqrt[n]{a}$（n、a 均为正整数）不是整数的话，它必是无理数。

5. 三 谈 整 除

如整数 n 是3的倍数，n 又是2的倍数，则 n 必是 $2\times3=6$ 的倍数。由此自然会发问，这一事实能否推广到一般情形？即已知 $a|n$，$b|n$，能否导出 $ab|n$？这个命题一般是不真的。举例以说明之：

$$4|12,\ 6|12 \quad 但\ 24\nmid 12$$❶

然而，在 a、b 之间若附加一定的条件后，命题就能成立。在有了公因数及互素的概念后，我们就可确切地回答这个问题。首先有

性质 9 若 $(a,b)=1$ 且 $b|ac$，那么 $b|c$。

证 因 $(a,b)=1$，由性质7知存在整数 k 与 l，使 $ak+$ $+bl=1$，即得 $ack+bcl=c$。由假设 $b|ac$，又 $b|bcl$，故得 $b|c$。

现在来回答上面提出的问题，这就是

性质 10 若 $a|c$，$b|c$，且 $(a,b)=1$，则 $ab|c$。

证 因 $a|c$，故有整数 q 使 $c=aq$。又因 $b|c$，即有 $b|aq$。再由假设 a、b 互素，按性质9得 $b|q$，所以 $ab|aq$，因之，$ab|c$。

下面我们讨论有关最小公倍数的一些问题。先引出

定义 若正整数 l 是 a 和 b 的倍数，就称 l 是 a、b 的一个公倍数。a、b 的诸公倍数中最小的一个，设为 m，叫做 a 和 b 的最小公倍数，记作 $[a,b]=m$。

---

❶ 记号 $\nmid$ 表示不能整除，$24\nmid 12$ 意即表示24不能整除12。

性质 11 设正整数 a、b 的最大公因数 $(a,b)=d$，那么它的最小公倍数

$$[a,b]=ab/(a,b)。$$

证 设 m' 是 a、b 的一个公倍数，即有正整数 k、k' 使 $m'=ak=bk'$。又因 $(a,b)=d$，故有正整数 a_1 和 b_1 使 $a=a_1d$，$b=b_1d$，代入上式得 $a_1kd=b_1k'd$，即有 $a_1k=b_1k'$，从而 $b_1|a_1k$。由习题 4 第 5 题知 $(a_1,b_1)=1$，故由性质 9，$b_1|k$，亦即有整数 t 使 $k=b_1t$。所以

$$m'=ak=ab_1t=\frac{ab}{(a,b)}t。\qquad (1)$$

对任一正整数 t，$abt/(a,b)$ 都是 a 和 b 的公倍数，所以(1)式给出了 a、b 的一切公倍数，因之，当 $t=1$ 时得最小公倍数。故证得

$$[a,b]=ab/(a,b)。$$

这一式子提供了求最小公倍数的一个具体计算公式。关于最小公倍数的性质在 §8 还要作进一步的讨论。现在我们利用性质 9、10 来解某些类型的整除性问题。

【例 1】 试证：相继三个整数的积能被 6 整除。

证 相继三个整数 $n-1$，n，$n+1$ 之中必有一偶数，也必有一个 3 的倍数(余数公式)。因 $(2,3)=1$，所以由性质 10，$2\times 3|(n-1)n(n+1)$，即能被 6 整除。证毕。

【例 2】 若 $2\nmid n$，$3\nmid n$，那么 $24|(n^2-1)$。

证 因 $2\nmid n$，即 n 为奇数，可记 $n=2k+1$，故有

$$\begin{aligned}(n^2-1)&=(n-1)(n+1)=2k(2k+2)\\&=4k(k+1)。\end{aligned}$$

由 §2 例 1 知 $2|k(k+1)$，故得 $8|(n^2-1)$。另一方面，相继三个整数 $n-1$，n，$n+1$ 必有一个是 3 的倍数，但已知 $3\nmid n$，因此可得 $3|(n^2-1)$。易知 $(3,8)=1$，从而按性质 10 得证

$24|(n^2-1)$。

【例 3】 试证：相继三个整数的立方和是 9 的倍数。

证 设相继的三个整数为 $n-1, n, n+1$,而

$$(n-1)^3+n^3+(n+1)^3=3n(n^2+2)$$
$$=3[n(n^2-1)+3n],$$

由例 1 已知 $3|n(n^2-1)$，所以证得 $9|[(n-1)^3+n^3+(n+1)^3]$。

【例 4】 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ 是整系数多项式，如 $10|f(2)$ 且 $10|f(5)$，那么 $10|f(10)$。

证 因

$$f(10)=a_0 10^n+a_1 10^{n-1}+\cdots+a_{n-1}10+a_n,$$

所以欲 $10|f(10)$ 只须证 $10|a_n$。

由 $10|f(2)$，有 $2|f(2)$，故得 $2|a_n$。同样，由 $10|f(5)$，有 $5|f(5)$，故得 $5|a_n$。易知 $(2,5)=1$，依性质 10 得 $10|a_n$。证毕。

【例 5】 怎样的正整数 n，使得数 $20^n+16^n-3^n-1$ 能被 323 整除？

解 先写出 $323=17\times19$。当 n 为正偶数时，即 $n=2k$，差 20^n-3^n 能被 $20-3=17$ 整除，又因

$$16^n-1=16^{2k}-1=256^k-1=(256-1)N$$
$$=17\times15\times N, \tag{2}$$

其中 N 是某正整数，即差 16^n-1 也被 17 整除。所以当 n 为偶数时，17 能整除 $20^n+16^n-3^n-1$。

另一方面，差 20^n-1 能被 $20-1=19$ 整除，又因

$$16^n-3^n=16^{2k}-3^{2k}=256^k-9^k$$
$$=(256-9)M=19\times13\times M,$$

其中 M 是某正整数，即差 16^n-3^n 也被 19 整除。所以当 n 为偶数时，19 能整除 $20^n+16^n-3^n-1$。易知 $(17,19)=1$，

结合两方面，由性质10，证得n为偶数时，$323=17\times19$能整除$20^n+16^n-3^n-1$。

考察n为正奇数的情况，即$n=2k+1$。易见差20^n-3^n能被$20-3=17$整除。但因

$$16^n-1=16^{2k+1}-1=16^{2k+1}-16+15$$
$$=16(16^{2k}-1)+15,$$

由(2)式，已知17能整除$16^{2k}-1$，而15与17是互素的，再利用习题1第4题可以推出：若两数b_1、b_2，有$a|b_1$而$a\nmid b_2$，那么$a\nmid(b_1+b_2)$，因此可得17不能整除它们的和16^n-1。同理可得n为奇数时，17不能整除$20^n+16^n-3^n-1$。所以此数也不能被323整除。

总起来，解得：当且仅当n为正偶数时，$20^n+16^n-3^n-1$能被323整除。

习 题 5

1. 试证：(i) 当n为偶数时，$48|(n^3-28n)$；

(ii) $12|n^2(n^2-1)$；

(iii) $24|n(n^2-1)(3n+2)$；

(iv) $30|n(n^2-49)(n^2+49)$。

2. 若$6|(a_1+a_2+a_3)$，证明$6|(a_1^3+a_2^3+a_3^3)$。

3. 若$2\nmid a_1$，$2\nmid a_2$，$3\nmid a_1$，$3\nmid a_2$，证明$24|(a_1^2-a_2^2)$。

4. 试证：$(1+2+\cdots+9)|(1^5+2^5+\cdots+9^5)$。

5. 证明下式：

$12|(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$。

6. 若k为正奇数，证明$6|(n^k-n)$。若n也为奇数，那么$24|(n^k-n)$。

7. 设 n 为正整数，证明 $(n+4)\nmid(n^2+8n+15)$。

8. 设 n 为正整数，证明 $7\nmid(2^n+1)$。

9. (i) 若 $(K, M)=1$，试证在数 $M, 2M, \cdots, kM$ 中任何两数之差不能被 K 整除；

(ii) 试证：对任给正整数 N，可在数 $M, 2M, \cdots, KM$ 中找到一数 lM，使得 $K\mid(lM+N)$。

10. 试证正整数 a、b 的最小公倍数 $[a, b]$ 满足关系式：

(i) $[a,a]=a$；

(ii) $[a,b]=[b,a]$；

(iii) $(a+b)[a,b]=b[a, a+b]$。

6. 组合数 C_n^k 与整除

在二项定理 $(a+b)^n$ 展开式中，每一项 a、b幂次前的系数称为二项系数。在学习排列和组合时，我们知道二项系数就是组合数，它是一个整数，指从 n 个不同对象中任取 $k(0\leqslant k\leqslant n)$ 个的取法，常记作 C_n^k 或 $\binom{n}{k}$。本节的内容着重说明怎样利用组合数及其性质，去解有关整除性的问题。

在第 5 节的例 1 中，我们已经看到三个相继整数的乘积 $(n-1)n(n+1)$ 是 6 的倍数，即 $3!\mid(n-1)n(n+1)$。其实，我们还可利用组合数获得更一般的结果，那就是

性质 12 相继 k 个整数的乘积能被 $k!$ 整除，亦即

$$k!\mid n(n-1)\cdots(n-k+1)。$$

证 当 n 为正整数，且 $n\geqslant k$ 时，注意到组合数 C_n^k 的意义，C_n^k 总是一个正整数。但另一方面，熟知有

$$C_n^k=n(n-1)\cdots(n-k+1)/k!$$

这就是说，相继 k 个正整数的乘积能被 $k!$ 整除。由此不难证明，对于 k 个整数的情形，命题也成立。

【例 1】 试证：$6\mid n(n-1)(2n-1)$。

证 注意到

$$n(n-1)(2n-1)=n(n-1)(n+1)+n(n-1)(n-2),$$

由性质 12，

$$3!\mid(n-1)n(n+1),3!\mid n(n-1)(n-2),$$

故得证

$$6 \mid n(n-1)(2n-1)。$$

【例 2】 试证：$120 \mid (n^5 - 5n^3 + 4n)$。

证 因为

$$n^5 - 5n^3 + 4n = n(n^2 - 1)(n^2 - 4)$$
$$= (n-2)(n-1)n(n+1)(n+2)$$

是 5 个相继整数的乘积，所以能被 $5! = 120$ 整除。

【例 3】 试证：$24 \mid n(n+2)(7n+1)(7n-1)$。

证 设法分化出一部分相继整数的乘积，

$$n(n+2)(7n+1)(7n-1) = n(n+2)(49n^2 - 1)$$
$$= n(n+2)(n^2 - 1) + 48n^3(n+2)$$
$$= (n-1)n(n+1)(n+2) + 48n^3(n+2),$$

上式最后一行第一项是 4 个相继整数的乘积，另一项是 24 的倍数，所以都能被 $4! = 24$ 整除，由此即得 24 整除 $n(n+2)(7n+1)(7n-1)$。

【例 4】 试证：$360 \mid n^2(n^2 - 1)(n^2 - 4)$。

证 因为

$$n^2(n^2 - 1)(n^2 - 4) = (n-2)(n-1)n^2(n+1)(n+2),$$

由性质 12，

$$5! \mid (n-2)(n-1)n(n+1)(n+2),$$

故

$$5! \mid n^2(n^2 - 1)(n^2 - 4),$$

更有

$$5 \cdot 4 \cdot 2 \cdot 1 \mid n^2(n^2 - 1)(n^2 - 4)。$$

另一方面

$$3 \mid (n-2)(n-1)n, \quad 3 \mid n(n+1)(n+2),$$

故

$$9 \mid n^2(n^2 - 1)(n^2 - 4)。$$

但$(40,9)=1$，结合两方面证得

$$360\mid n^2(n^2-1)(n^2-4)。$$

【例 5】 证明：对任何整数n，多项式

$$f(n)=\frac{1}{5}n^5-\frac{2}{3}n^3-\frac{8}{15}n$$

取整数值。

证 先写

$$f(n)=\frac{1}{15}(3n^5-10n^3-8n)$$

$$=\frac{1}{15}[3(n^5-5n^3+4n)+5(n^3-n)-15n]$$

$$=\frac{1}{5}(n^5-5n^3+4n)+\frac{1}{3}(n-1)n(n+1)-n,$$

由例 2 及性质 12，可知上式右边各项都是整值。

【例 6】 对任何正整数n，要使 $n+1$ 个组合数 C_n^0，C_n^1，$\cdots$，C_n^n 都为奇数的充要条件是：n 有着 $n=2^k-1$ 的形式。

证 用数学归纳法证明，当$n\leqslant 7$时，直接验证可知，仅在$n=1=2^1-1$，$n=3=2^2-1$，$n=7=2^3-1$时，组合数 $C_n^l(0\leqslant l\leqslant n)$ 都是奇数。假设对于$<n$的情形命题成立。

在n情形，全体组合数C_n^l就是

$$1,\ n,\ \frac{n(n-1)}{2!},\cdots,\frac{n(n-1)\cdots(n-l+1)}{l!},\cdots,n,1,$$

要使这些数都为奇数，首先，第二项及倒数第二项的n应是奇数，即 $n=2m+1$。另外，在其余各项的分子、分母中，把奇数因子去掉后，余下部分让 $n=2m+1$ 代入，恰得

$$\frac{m}{1},\ \frac{m(m-1)}{1\times 2},\ \cdots,\ \frac{m}{1},$$

要使全体 C_n^l 都是奇数，由性质 3 知它们也应全是奇数，而它们恰是 $m(<n)$ 时的全体 $C_m^l\ (0<l<m)$。由归纳假设，要使它们都是奇数的充要条件是 $m=2^k-1$ 形式，此时

$$n=2m+1=2(2^k-1)+1=2^{k+1}-1。$$

这就证明了命题成立。

习　题　6

1. 试证：$6\mid n(2n+1)(n-5)$。

2. 试证：$36\mid n^2(2n^4+3n^3-n^2-3n-1)$。

3. 试证：$8640\mid n^9-6n^7+9n^5-4n^3$。

4. 相继的 k 个偶数的乘积必能被 $2^k\cdot k!$ 整除。

5. 证明：$f(n)=\frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$ 是整值多项式。

6. 证明：$f(n)=\frac{2}{5}n^5-\frac{1}{3}n^3-\frac{1}{15}n$ 是整值多项式。

7. 设 $(m,n)=1$，证明 $(m+n-1)!$ 能被 $m!n!$ 整除。

8. 证明：若 $a+b+\cdots+k\leqslant n$，则 $\frac{n!}{a!b!\cdots k!}$ 为整数。

9.* 证明：对正整数 $n,m(>1)$，$k\leqslant n+1$，m^{n-k+1} 能整除 $C_{m^n}^k$。

7. 素　　数

数 1 只有一个正因数1。显然，任何大于 1 的正整数 n 至少有 1 及 n 两个正因数。有的数恰好只有两个正因数，如 2，3，5，7，……等等，有的则有多于两个正因数，如 4，6，8，9，…等等。

定义　若正整数 p 恰好只有 1 及本身 p 两个正因数，则称 p 是素数或质数。若正整数 n 有多于两个正因数，则称 n 是合数。如数 n 的一个因数 p 是素数，则称 p 是 n 的一个素因数。

今后，我们常用 q，p，p_1，p_2，…表示素数。依定义，全体正整数按其正因数的多少可分成三类。

（1）1：只有一个正因数，

（2）全体素数：有且仅有两个正因数，

（3）全体合数：有多于两个正因数。

特别请注意，1 既不是素数也不是合数。

性质 13　设 n 是任一大于 1 的整数，那么 n 的大于 1 的最小正因数 p 必是素数，且当 n 为合数时，$p \leqslant \sqrt{n}$。

证　用反证法先证命题的第一部分。如 p 不是素数，由定义，它除 1 及本身外，还有一个正因数 q，因此 $1 < q < p$，且 $q|p$。又由假设 $p|n$，所以 $q|n$，即 q 也是 n 的大于 1 的因数，这与 p 是 n 的大于 1 的最小正因数的假设相矛盾，故 p 是素数。

证另一部分，当 n 是合数时，记 $n = pm$，此时 $m > 1$，因不然若 $m = 1$，就有 $n = p$ 是素数，由于 p 是 n 的大于 1 的

最小正因数，所以 $p \leqslant m$，从而 $p^2 \leqslant pm = n$，得证

$$p \leqslant \sqrt{n}。$$

从性质 13 可推出

系 设整数 $n > 1$，若所有 $\leqslant n$ 的素数都不能整除 n，那么 n 是素数。

性质 14 任给素数 p，正整数 n，那么或者 $p|n$ 或者 $(p,n) = 1$，两者有且仅有一个成立。

证 因为 $(p, n)|p$，由于 p 是素数，所以或 $(p, n) = 1$，或 $(p,n) = p$ 有且仅有一个成立，这就是说，或 $(p, n) = 1$，或 $p|n$ 两者必居其一，不得兼有。

性质 15 设 n,m 为正整数，p 为素数，若 $p|mn$，那么或 $p|n$，或 $p|m$，两者至少有一成立。

证 用反证法。若不然，两者都不成立，即 $p\nmid n$ 且 $p\nmid m$，那么由性质 14，$(p, n) = (p, m) = 1$，由 § 4 例 4 可知 $(p, nm) = 1$，这与 $p|nm$ 矛盾。证毕。

性质 16 素数的个数是无穷的。

证 用反证法。设若只有有限个素数，记为 $p_1, p_2, \cdots, p_k$，即除 $p_1, p_2, \cdots, p_k$ 外无另外的素数。讨论数 $p_1p_2\cdots p_k + 1 = N$。因 $N > 1$，由性质 13，N 有一个大于 1 的素因数 p。现证这个素数 p 异于 $p_1, p_2, \cdots, p_k$ 中的任何一个。事实上，若 $p = p_i (1 \leqslant i \leqslant k)$，那么 $p|p_1p_2\cdots p_k$，又 $p|N$，所以 $p|1$，这与 p 是素数相矛盾。因此，p 是素数 $p_1, p_2, \cdots, p_k$ 以外的一个素数，与假设矛盾。这样，证得素数个数是无穷的。

利用性质 13，在给定正整数 n 以后，我们可以提供一个求出不大于 n 的所有素数的方法。例如要求不大于 50 的全体素数，由于不大于 $\sqrt{50}(<8)$ 的素数是 2、3、5、7，故依性质 13，在 2，3，4，……50 中的合数必有一素因数为 2，或 3，或 5，或 7，留下 2，3，5，7 外，顺次划去它们的倍数，即先划去 2

的倍数，再划去 3 的倍数，再顺次划去 5 的及 7 的倍数：

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~

19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~

~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~

余下的数 2、3、5、7、11、13、17、19、23、29、31、37、41、43、47 就是不超过 50 的全体素数。用这种方法逐步地把素数筛选出来。此法称为爱拉脱斯染纳（Eratosthenes）筛法。

用筛法可以制成素数表。虽然素数是无限的，但由于筛法的局限和书写上的限制，制出的素数表总是有限的。对于超出素数表范围的一个大数，要判断它是不是素数仍然是困难的，并没有什么统一的方法。有许多这方面的问题迄今未获解决。

现在我们来看一些例子。

【例 1】 若 2^p-1 是素数，那么 p 是素数。

证 用反证法。若 p 不是素数，可设 $p=kl, 1<k<p$，那么 $2^p-1=(2^k)^l-1$ 有因数 2^k-1，而 $2^p-1>2^k-1>1$，所以 2^p-1 就不是素数。因此反证得 p 必是素数。

【例 2】 试证：与 $1, 2, 3, \cdots\cdots, n$ 互素的最小正整数 N 是素数。

证 若不然，设 N 是合数即可写成 $N=pq$，$1<p<N$。对任一整数 $k(1\leqslant k\leqslant n)$，$(p, k)|p$，故 $(p, k)|N$。又 $(p,k)|k$，从而 $(p, k)|(N, k)=1$，即得 $(p, k)=1$，这就是说，p 也是与 $1,2,\cdots\cdots,n$ 互素的正整数，但 $p<N$，这和 N 的最小性假设矛盾。因此证得 N 是素数。

【例 3】 证明：数 $1\overbrace{00\cdots\cdots0}^{1985}1$ 是合数。

证 $1\overbrace{00\cdots\cdots0}^{1985}1=10^{1986}+1=(10^{662})^3+1$，易见它有因数

$10^{662}+1$。

【例4】 试证：$F_5=2^{2^5}+1$是合数（$F_n=2^{2^n}+1$ 型数称为费尔马（Fermat）数）。

证 这是因为

$$
\begin{aligned}
F_5 &= 2^{2^5}+1=2^4(2^7)^4+1\\
&=(2^7\times 5-5^4+1)(2^7)^4+1\\
&=(1+2^7\times 5)(2^7)^4+1-(2^7\times 5)^4\\
&=(1+2^7\times 5)\{(2^7)^4+(1-5\times 2^7)[1+(5\times 2^7)^2]\}\\
&=641\times 6700417。
\end{aligned}
$$

【例5】 试证：对任何正整数 n，$289\nmid(4n^2-2n+13)$。

证 首先注意到 $289=17^2$，而

$$4n^2-2n+13=(2n-9)^2+17(2n-4)。\qquad (1)$$

用反证法，若 $289\mid(4n^2-2n+13)$，那么 $17\mid(4n^2-2n+13)$。注意到(1)，可得 $17\mid(2n-9)^2$，因 17 是素数，由性质 15，$17\mid(2n-9)$。再由(1)，可得 $289\mid 17(2n-4)$，故知 $17\mid(2n-4)$。这样，应用性质 2，便出现 $17\mid[(2n-4)-(2n-9)]=5$，显然这是不可能的，矛盾。得证命题成立。

【例6】 (i) 若素数 p 除以 30 后的余数 $p'\neq 1$，则 p' 必为素数；

(ii) 若素数 $p\geqslant 7$，则 p^2 除以 30 的余数必为 1 或 19。

证 (i) 设 $p=30k+p'$，$p'\neq 1$。因 p 是素数，故 p' 不能是 2,3,5 的倍数，且 $1<p'<30$。由性质 13，若 p' 为合数，那么必有一个不大于 $\sqrt{p'}<\sqrt{30}<6$ 的素因数，它们就是 2,3,5，这就引出了矛盾。故 p' 只能是素数，即 7，11，13，17，19，23，29。

(ii) 由(i)得，p 只可表成 $30k+1$，$30k+7$，$30k+11$，

$30k+13$，$30k+17$，$30k+19$，$30k+23$，$30k+29$。一一验证后，可知 p^2 除以 30 后的余数分别为 1,19,1,19,19,1,19,1。

习　题　7

1. 设 a、b 是整数，p 为素数，证明 $p\mid[(a+b)^p-a^p-b^p]$。

2. 试证：对大于 1 的整数 n，n^4+4 是合数。

3. 设 $p>5$，若 p 及 $2p+1$ 均为素数，则 $4p+1$ 必是合数。

4. 设 p 是一个大于 3 的素数，那么 p^2 被 12 除的余数必为 1。

5. 设正整数 $m,n(>1)$ 被 3 除的余数分别为 1 及 2，正整数 $a\neq 3$，试证 $a,a+m,a+n$ 不可能都为素数。

6. 试求：能使 p 和 $8p^2+1$ 都是素数的一切 p。

7. 试求：能使 $p,p+10$，$p+14$ 都是素数的一切 p。

8. 对任何正整数 n，试证 $121\nmid(n^2+3n+5)$。

9.* 证明：当 $n>2$ 时，n 与 $n!$ 之间一定有一个素数。

10.* 设在区间 $[0,1]$ 上的点 $0=x_0<x_1<\cdots<x_n=1$ 把单位区间分为 n 个(不一定等长的)部分。证明或否定下述论断：存在着这样的合数 m，使得每一区间 $[x_i,x_{i+1}]$ $(i=0,1,2,\cdots,n-1)$ 中至少含有一个型如 $\frac{l}{m}$ 的不可约分数。

8. 整数的分解

性质 17 （算术基本定理） 任一大于 1 的正整数 n 都可以分解成若干个素数的连乘积

$$n = p_1p_2\cdots p_l \quad (p_1 \leqslant p_2 \leqslant \cdots \leqslant p_l), \tag{1}$$

并且这样的分解是唯一的，即若另有

$$n = q_1q_2\cdots q_m \quad (q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m), \tag{2}$$

其中 $q_1, q_2, \cdots, q_m$ 是素数，那么 $l = m$，$p_i = q_i$ $(i = 1, 2, \cdots, l)$。

证 先证明(1)式的存在性。对 n 用数学归纳法。当 $n = 2$ 时，(1)式显然正确。假设(1)式对于小于 n 的正整数成立。现证对于 n，(1)式亦成立。若 n 是素数，(1)式显然是成立的。若 n 是合数，那么 n 有因数 t，$1 < t < n$，使得 $n = ts$，此时也有 $1 < s < n$，由归纳假设，对于 t 和 s，有

$$t = p_1'p_2'\cdots p_j', \quad s = p_{j+1}'p_{j+2}'\cdots p_l',$$

所以

$$n = ts = p_1'p_2'\cdots p_j'p_{j+1}'\cdots p_l'。$$

在适当改变上式中诸 p' 的顺序之后，得(1)式对 n 成立。这就证明了对于任何正整数 n，(1)式成立。

现证(1)式的唯一性。如果对 n 的表示除(1)式以外还有(2)式也能适合，即

$$n = p_1p_2\cdots p_l = q_1q_2\cdots q_m。\tag{3}$$

由此，$p_1 | q_1q_2\cdots q_m$，按性质 15 可以推得，有 q_j 使 $p_1 | q_j$，由于 p_1 和 q_j 都是素数，所以 $p_1 = q_j$，从而有 $q_1 \leqslant q_j = p_1$；同理，$q_1 | p_1p_2\cdots p_l$，所以有 p_k 使 $q_1 = p_k$，从而有 $p_1 \leqslant p_k = q_1$。

因此，结合两者得 $p_1 = q_1$。这样，由(3)，$p_2p_3\cdots p_l = q_2q_3\cdots q_m$。再用归纳法不难获得 $l = m$，$p_i = q_i$，$i = 1, 2, \cdots, l$。证毕。

系 任一大于 1 的正整数 n 可以唯一地分解成

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \tag{4}$$

其中 $p_1 < p_2 < \cdots < p_k$ 是素数，$\alpha_i(i = 1, \cdots, k)$是正整数。(4)式称为正整数 n 的标准分解式。有时为了方便，我们也允许幂指数 α_i 可以是零。

性质 18 若正整数 $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，那么 n 的任一正因数 d 都有形式

$$d = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}, \quad 0 \leqslant \beta_j \leqslant \alpha_j。$$

证 对 d 的标准分解式中每一个素因数 p，自然有 $p|d$。因为 $d|n$，所以 $p|n$。因此，p 也应是 n 的标准分解式中的素因数，而且在 d 中出现的指数 β_i 不大于 α_i，即 $\beta_i \leqslant \alpha_i$。证毕。

性质 19 若正整数

$$m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \ n = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}, \ \alpha_i \geqslant 0, \ \beta_i \geqslant 0, \quad i = 1, 2, \cdots, k。$$

那么

$$(m, n) = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}, \tag{5}$$

$$[m, n] = p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}, \tag{6}$$

其中 $\gamma_i = \min(\alpha_i, \beta_i)$，表示 α_i, β_i 中较小的一个数；$\delta_i = \max(\alpha_i, \beta_i)$，表示 α_i, β_i 中较大的一个数。

证 由性质 18，最大公因数 (m, n) 是一个因数，故有(5)的形式，其中 $\gamma_i \leqslant \alpha_i, \gamma_i \leqslant \beta_i$，由于最大公因数的性质，可取 $\gamma_i = \min(\alpha_i, \beta_i)$，又由性质 11，$[m, n] = mn/(m, n)$，所以最小公倍数有(6)式那样的标准分解式，且 $\delta_i = \alpha_i + \beta_i - \gamma_i$，因 $\gamma_i = \min(\alpha_i, \beta_i)$，不妨设 $\alpha_i \leqslant \beta_i$，即 $\gamma_i = \min(\alpha_i, \beta_i) =$

α_i，那么 $\delta_i = \beta_i = \max(\alpha_i, \beta_i)$。

性质 20 若有正整数

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad 0 < \alpha_i, \quad i = 1, 2, \cdots, k,$$

那么 n 的正因数的个数

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)。$$

证 由性质 18，n 的因数 d 都有形式 $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$，$0 \leqslant \beta_i \leqslant \alpha_i$。由性质 17 可知，对每一组不同的 $\beta_1, \beta_2, \cdots, \beta_k$ 对应着不同的因数 d，而每一 β_i 可取 $0, 1, \cdots\cdots, \alpha_i$ 等 $\alpha_i + 1$ 个值，所以不同的 $(\beta_1, \beta_2, \cdots, \beta_k)$ 的组数为 $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ 个，由此证得 n 的因数的个数

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)。$$

现在我们举一些例子。

【例 1】 若 $2^n + 1$ 为素数，则 $n = 2^k$。

证 若 n 的标准分解式为 $n = 2^k p_2^{\alpha_2} \cdots p_l^{\alpha_l}$，因为 $p_2, \cdots, p_l$ 都是奇素数，我们可设 $p_2^{\alpha_2} \cdots p_l^{\alpha_l} = P$。即 $n = 2^k P$，$2 \nmid P$。如果还有 $\alpha_2, \cdots, \alpha_l$ 不全为 0，则有奇数 $P > 1$，从而就有

$$2^n + 1 = 2^{2^k P} + 1 = (2^{2^k})^P + 1 = (2^{2^k} + 1)Q,$$

其中 Q 为大于 1 的整数，与 $2^n + 1$ 为素数的假设矛盾。 证毕。

这一例子告诉我们，若 $2^n + 1$ 形的数是素数的话，那么它必是某一费尔马数 $F_k = 2^{2^k} + 1$。反过来，是否每一费尔马数都是素数呢？在 §7 例 4 中已告诉我们 F_5 就不是素数。

从理论上讲，任一正整数 n 都有标准分解式(4)，但正如要确定一个正整数是否是素数一样，当给定一个正整数 N 很大时，要具体写出它的素因数标准分解式是不容易的。

【例 2】 试分解

$$13717421 = 761^2 + 7 \times 1370^2 = 439^2 + 7 \times 1390^2$$

为素因数的乘积。

解 一般地说，当 $N = x_1^2 + dy_1^2 = x_2^2 + dy_2^2$ 时，必有 $x_1^2 - x_2^2 = d(y_2^2 - y_1^2)$，

即
$$\frac{x_1 - x_2}{y_2 - y_1} = d\frac{y_1 + y_2}{x_1 + x_2}$$

令 $y_1 + y_2 = u \cdot s \qquad x_1 + x_2 = v \cdot s$

则
$$\frac{x_1 - x_2}{y_2 - y_1} = d\frac{u}{v} \qquad (u, v) = 1$$

现 $d = 7$ 与 $(x_1 + x_2) = 761 + 439 = 1200$ 互素

令 $(y_2 - y_1)/v = t$

则
$$x_1 - x_2 = dut$$
$$y_2 - y_1 = vt$$

可得
$$N = \frac{1}{4}[(dut + vs)^2 + d(us - vt)^2]$$
$$= \frac{1}{4}(du^2 + v^2)(dt^2 + s^2)。$$

解之得 $d = 7$，$u = 23$，$v = 10$，$t = 2$，$s = 120$，代入得 $N = 3803 \times 3607$，直接验算或查素数表知 3803 和 3607 为素数。

【例 3】 试找出所有奇数 n，使 $n^2 | (n - 1)!$。

解 当 $n = p$ 为素数时，显然 $p \nmid (p - 1)!$，更有 $p^2 \nmid (p - 1)!$。又当 $n = 9$ 时，直接验算知 $9^2 = 3^4 \nmid 8!$。现证其余情形都有 $n^2 | (n - 1)!$。

当 $n = ab$，且 $1 < a < n$，$1 < b < n$，$a \neq b$ 时，因 n 为奇数，所以 a，b 为奇数。

只要讨论 $3 \leqslant a$，$3 \leqslant b$ 情况。此时 $3a \leqslant ab = n$，$3b \leqslant ab = n$。从而 $2a < 3a \leqslant n$。故在 $1, 2, 3, \cdots, (n - 1)$ 中必有 a 及 $2a$。又因假定 $a \neq b$，同理可知，在 $1, 2, 3, \cdots, (n-1)$

中还有 b 及 $2b$。故在 $(n-1)!=1,2\cdots(ab-1)$ 中有 a，$2a$，b，$2b$ 四个互不相同的因数，因此，$(n-1)!$ 能被 $a^2b^2=n^2$ 整除。

当 $a=b$ 时，只要 a，b 不是素数，我们总可以把 $n=ab$ 化成 $n=a'b'$，$a'\neq b'$ 的情况。

最后讨论 $n=p^2$，p 为素数且 $p\geqslant 5$ 的情况。此时，$4p<5p\leqslant p^2=n$，所以 $4p\leqslant n-1$，即在 $(n-1)!$ 中有 p，$2p$，$3p$，$4p$ 四个互不相同的因数，因此 $(n-1)!$ 能被 $n^2=p^4$ 整除。

因此，只有所有大于 9 的奇合数 n 满足 $n^2|(n-1)!$。

【例 4】 证明 $4m+3$ 型的素数有无穷多个。

证 反证法。若不然，$4m+3$ 型的素数只有有限个，设为 p_1，p_2，$\cdots$，p_k 等 k 个。注意到 $N=4p_1p_2\cdots p_k-1=4m+3$。因 $4m+1$ 型的数的乘积仍是 $4m+1$ 型的，所以在 $4m+3$ 型的数 N 中必有一个 $4m+3$ 型的素因数 q。我们说 q 与 p_1，$\cdots$，p_k 是互不相等的。事实上，如果 q 与 p_j $(1\leqslant j\leqslant k)$ 相等，那么 $q|4p_1p_2\cdots p_k$，又 $q|N$，所以 $q|1$，矛盾。这就是说，q 是与 p_1，$\cdots$，p_k 不同的另一个 $4m+3$ 型素数，这又与 p_1，$\cdots$，p_k 是全部 $4m+3$ 型的素数的假设矛盾。因此，得证 $4m+3$ 型的素数有无穷多个。

习 题 8

1. 试求 1000027 的素因数分解式。

2. 设正整数 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，试证：$\sqrt[m]{n}$ 为正整数的充要条件是 $m|\alpha_i$，$i=1,2,\cdots,k$。

3. 设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$\alpha_i\geqslant 0$，$m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$，

$\beta_i \geqslant 0$，试证：$\log_m n$ 为有理数的充要条件是所有的 α_i，β_i 同时为正，且 $\beta_1/\alpha_1 = \beta_2/\alpha_2 = \cdots = \beta_k/\alpha_k = r/s$，$r$ 与 s 为某正整数。

4. 试证 $6m+5$ 型的素数有无穷多个。

5. 证明：如果 m 为 >1 的正整数，那么当且仅当 m 为大于 5 的合数时，$m \mid (m-1)!$。

* **6.** 试证：

$$S_n = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

不是整数，其中 $n \geqslant 2$。[提示：设 k 是满足 $2^k \leqslant n$ 的最大整数，P 为所有 $\leqslant n$ 的奇数的乘积，讨论 $2^{k-1}PS_n$]。

* **7.** 证明 $2^n \mid C_{2^n}^{2^k-1}$，但 $2^{n+1} \nmid C_{2^n}^{2^k-1}$。

9. 整数的数码特征 整除性判别法

要判别一个数是合数还是素数，或要把一个整数分解成素因数的乘积，这与判别一个正整数 a 能否整除整数 n 是直接相关联的。虽然我们已经讨论过若干整除性的基本性质，但要是给定两个整数，如 37 与 13717421，问 37 能否整除后者，那就没有一个方便的法则可循，而只能具体去算，看它能否整除。现在我们提出这样的问题：能否从数的各个数码间的关系给出一个检验整除性的判别法？回想到已有的一些特殊的整数判别法就是利用数码之间的关系而建立的，看来这还是有可能办到的。本节就想在这方面作些探讨。

我们先引出几个记号：任一正整数 n 可以写成

$$n = 10^m a_m + 10^{m-1} a_{m-1} + \cdots + 10 a_1 + a_0,$$

其中 $0 \leqslant a_i \leqslant 9$，称 a_m 为 n 的首位数码，a_0 为末位数码或个位数，也写 $n = \overline{a_m a_{m-1} \cdots a_1 a_0}$。

记 n 的数码和为

$$S_1(n) = a_m + a_{m-1} + \cdots + a_1 + a_0。$$

若把正整数 n 自末位数码 a_0 向左数起，每 k 个数码为一节，最后剩下若有不足 k 个的数码，也作为一节，设共得 $t+1$ 节，各记为 $A_{0,k}(n)$，$A_{1,k}(n)$，$\cdots$，$A_{t,k}(n)$，它们的和记为

$$S_k(n) = A_{0,k}(n) + A_{1,k}(n) + \cdots + A_{t,k}(n)。$$

例如对于数 13717421，取 $k=3$，此时，$A_{0,3}(13717421) = A_{0,3} = 421$，$A_{1,3} = 717$，$A_{2,3} = 13$，故 $S_3(13717421) = 421 + 717 + 13 = 1151$。

性质 21 设 $d \mid 10^k$，那么 $d \mid n$ 充要条件是 $d \mid A_{0,k}(n)$。

证 因为 $n - A_{0,k}(n) = 10^k(10^{m-k}a_m + \cdots + 10a_{k+1} + a_k)$，故由假设 $d|10^k$，即得 $d|n$ 当且仅当 $d|A_{0,k}(n)$。

由此性质，便可给出能被 $d = 2^i5^j$ 型数整除的判别法，今举例说明之。

【例 1】 (i) 3587628 能否被 8 整除？(ii) 473238625 能否被 125 整除？(iii) 7584370 能否被 250 整除？

解 (i) 因 $8|10^3$，所以只须考察 8 能否整除 628，但 $8\nmid 628$，故 $8\nmid 3587628$。

(ii) 因 $125|10^3$，而 $125|625$，故 $125|473238625$。

(iii) 因 $250|10^3$，而 $250\nmid 370$，故 $250\nmid 7584370$。

性质 22 (i) 设 $d|(10^k - 1)$，那么 $d|n$ 的充要条件是 $d|S_k(n)$。

(ii) 设 $d|(10^k + 1)$，那么 $d|n$ 的充要条件是 $d|\tilde{S}_k(n)$，其中

$$\tilde{S}_k(n) = A_{0,k} - A_{1,k} + \cdots + (-1)^t A_{t,k}。$$

证 (i) 因为

$$\begin{aligned} n - S_k(n) &= 10^{tk}A_{t,k} + 10^{(t-1)k}A_{t-1,k} + \cdots \\ &\quad + 10^k A_{1,k} + A_{0,k} - (A_{t,k} \\ &\quad + A_{t-1,k} + \cdots + A_{1,k} + A_{0,k}) \\ &= (10^{tk} - 1)A_{t,k} + (10^{(t-1)k} - 1) \\ &\quad \times A_{t-1,k} + \cdots + (10^k - 1)A_{1,k}。\end{aligned}$$

由假设 $d|(10^k - 1)$，故 $d|[n - S_k(n)]$，因此，$d|n$ 当且仅当 $d|S_k(n)$。

(ii) 因为

$$\begin{aligned} n - \tilde{S}_k(n) &= A_{0,k} + 10^k A_{1,k} + \cdots + 10^{tk}A_{t,k} \\ &\quad - [A_{0,k} - A_{1,k} + \cdots + (-1)^t A_{t,k}] \\ &= (10^k + 1)A_{1,k} + (10^{2k} - 1)A_{2,k} \\ &\quad + \cdots + [10^{tk} - (-1)^t]A_{t,k}。\end{aligned}$$

由假设 $d|(10^k+1)$，而 $(10^k+1)|[10^{jk}-(-1)^j]$，所以 $d|[n-\tilde{S}_k(n)]$，因此，$d|n$ 当且仅当 $d|\tilde{S}_k(n)$。

系 1 $9|n$ 当且仅当 $9|S_1(n)$。

事实上，因 $9=10-1$，由 (i) 即得。

系 2 $11|n$ 当且仅当 $11|\tilde{S}_1(n)$。

事实上，因 $11=10+1$，由 (ii) 即得。

系 1、系2 都是我们已经熟知的结果。

【例 2】 (i) 13717421 能否被 37 整除？(ii) 7481329 能否被 7 整除？

解 (i) 因 $10^3-1=999=3^3\times37$，即 $37|(10^3-1)$，所以只需考察是否有 $37|S_3(13717421)$，我们有

$$S_3(13717421)=13+717+421=37\times31+4,$$

因此 $37\nmid S_3(13717421)$，所以 37 不能整除 13717421。

(ii) 因 $10^3+1=1001=7\times11\times13$，即 $7|(10^3+1)$，所以只需考察是否有 $7|\tilde{S}_3(7481329)$，而

$$\tilde{S}_3(7481329)=329-481+7=-145,$$

$7\nmid145$，所以 $7\nmid7481329$。

现在我们通过例子再来讨论整数数码的另一些特性。

【例 3】 若 $S_1(n)=S_1(2n)$，则 $9|n$。

证 数 n 乘以 2 时，某些数码有进位当且仅当该位数码 $\geqslant5$。而每次进位使得 $S_1(2n)$ 较 $2S_1(n)$ 少一个 9。设 n 乘 2 时有 l 个进位，那么 $S_1(2n)=2S_1(n)-9l$。由假设 $S_1(2n)=S_1(n)$，故得 $S_1(n)=9l$，由是 $9|S_1(n)$，再根据系 1 得 $9|n$。

【例 4】 设一个六位数 N，它的前三位数码组成的数 a 与它的后三位数码组成的数 b 之差 $b-a$ 能被 7 整除，试证 $7|N$。

解 此时

$$N = 1000 \times a + b = 1001 \times a + (b - a)。$$

因为 $7|1001$，再依假设 $7|(b-a)$，所以 $7|N$。

【例 5】 由 81 个数码 1 组成的 81 位数 N 能否被 81 整除？

解 分每 9 个数码为一节，共有 9 节，且每节全都相同。由性质 22 的系 1，$9|A_{0,9}(n)=A_{i,9}(n)$，$i=1,2,\cdots,8$。因此，$81|9A_{0,9}(n)$，即 $81|S_9(N)$，又 $81|(10^9-1)$，由性质 22(i)，故知 $81|N$。

【例 6】 哪些正整数当划去它的个位数码时恰好缩小了原正整数的整数倍？试具体给出这些数。

解 显然，以 0 结尾的正整数都满足这一性质。此外它只能是两位数。因不然，设 $N=\overline{a_m a_{m-1}\cdots a_1 a_0}$，因 $a_0 \neq 0$，$m \geq 2$，此时若有整数 k，使

$$\overline{a_m a_{m-1}\cdots a_1} \times k = \overline{a_m a_{m-1}\cdots a_1 a_0} = \overline{a_m\cdots a_1} \times 10 + a_0,$$

那么就得 $k = 10 + (a_0/\overline{a_m\cdots a_1})$，当 $a_0 \neq 0$，$m \geq 2$ 时，右边为分数，而左边却是整数，矛盾。

对于两位数 $\overline{a_1 a_0}$ $(a_0 \neq 0)$，由 $k = 10 + (a_0/a_1)$，只要 a_0/a_1 能取到整数值 $1,2,\cdots,9$，便有解。解之，得不是 0 结尾的两位数有：11，22，…，99；12，24，36，48；13，26，39；14，28；15，16，17，18，19。

【例 7】 由 1，2，3，4，5，6 能否组成各位数码不重复的而又能被 11 整除的六位数？

解 不能。若不然，记所组成的六位数为 $n=\overline{a_6 a_5\cdots a_1}$。由性质 22 系 2，$11|n$ 当且仅当 $11|\tilde{S}_1(n) = a_1 - a_2 + a_3 - a_4 + a_5 - a_6$，即 $a_1 - a_2 + a_3 - a_4 + a_5 - a_6 = 11k$，因为给定的六个数码之和是 21，故 k 只能取 0 或 1，所以

$$S_1(n) = a_1 + a_2 + a_3 + a_4 + a_5 + a_6$$
$$= 11k + 2\times(a_2 + a_4 + a_6)。$$

当 $k=0$ 时，因 $S_1(n)=21$，故 $2\times(a_2+a_4+a_6)=21$，矛盾。当 $k=1$ 时，$2(a_2+a_4+a_6)=10$，$a_2+a_4+a_6=5$，而在 1,2,3,4,5,6 中任三数之和 $\geqslant 6$，所以也无解。

【例 8】 试证：数 n^5 的末位数码与 n 的末位数码是相同的。

证 n 的末位数码 $a_0=0$ 或 5 时显然成立。

(i) $a_0=1,3,7,9$ 时，a_0^4 的末位数码为 1，所以 $a_0^5=a_0^4\times a_0$ 的末位数码与 a_0 相同。

(ii) $a_0=2,4,6,8$ 时，a_0^4 的末位数码都是 6，所以 $a_0^5=a_0^4\cdot a_0$ 的末位数码与 $6a_0=5a_0+a_0$ 的末位数码相同，因 $5a_0$ 末位数码为 0，因此，a_0^5 与 a_0 的末位数码相同。

总起来，对于任何的 n，n^5 与 n 的末位数码相同。

【例 9】 试求出满足下列两条件的不超过 10000 的所有素数：

(i) p 的数码任意排列后所得之数仍是一个素数，

(ii) p 的数码积与数码和是一个素数或 1。

解 容易看到 2, 3, 5, 7, 11 等五个素数均满足条件 (i) 和 (ii)。此外，由 (i) 可知，$p=a_na_{n-1}\cdots a_1a_0$ 的数码 a_n, $a_{n-1},\cdots,a_1,a_0$ 中不能含有 2,4,6,8,0 及 5，否则的话，把它们调换到末位时，就是合数了，所以它们只能是 1,3,7,9。再由 (ii)，数码个数不能是偶数，不然的话，其和必为大于 2 的偶数(偶数个奇数之和一定是偶数)，这样，就不满足 (ii)。最后，数码中异于 1 的个数不能多于 1 个，否则其积就不是素数。因之，只需考察至多除一个数码外全是 1 的诸数中，有哪些是满足 (i)、(ii) 的而又不超过 10000 的素数。此时因为数码总个数为奇数，故只能为有二个 1 型的数。直接验算共有 113,131,311 等三个，它们都是素数。因此，满足题意条件的素数只有 2,3,5,7,11,113,131,311 等八个。

随着电子数字计算机的蓬勃发展，除了最常用的十进位制以外，二进位制，八进位制乃至十六进位制的记数法已被广泛采用。限于本书的讨论范围，我们不打算介绍一般的 b 进位制的详细内容，而仅就 b 进位制的整除准则作扼要的简介。

给定一个自然数 b（依此作为 b 进位制的基），可将正整数 n 唯一地表示为下列形式

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

其中 $a_i (i = 0, 1, \cdots, k)$ 等于 $0, 1, \cdots, b-1$ 中的某一个数。这些数写成

$$\overline{a_k a_{k-1} \cdots a_1 a_0},$$

就称它是自然数 n 的 b 进位表示。

在性质 22 的系 1 和系 2，我们给出 $9|n$ 和 $11|n$ 的充要条件，对于 b 进位制，也有相仿的准则。

系 1′ 要使正整数 n 能被 $b-1$ 整除的充要条件是：它的 b 进位表示式中各数码 a_i 之和能被 $(b-1)$ 整除。

系 2′ 要使正整数 n 能被 $b+1$ 整除的充要条件是：它的 b 进位表示式中奇数位各数码和与偶数位各数码和之差能被 $b+1$ 整除。

证明可仿效性质 22 的证，留给读者作为练习。

【例 10】 试证：对于任何 b 进位制中的三位数 $\overline{aaa}$ 都不能满足关系式 $\overline{aaa} = a^3$。

证 对某 b 进位表示中如有 $ab^2 + ab + a = a^3$，则有 $b^2 + b + 1 = a^2$。但我们知道，数的 b 进位表示式中的数码 a_i 都是小于 b 的，即 $a_i < b$，因此，给定的关系式对任何 a 和 b 都不能成立。

习 题 9

1. 试求数列 $1, 2, \cdots, (10^n - 1)$ 的一切数中的各个数码

之总和。

2. 下列事实是否成立：

(i) 25 整除 17445；(ii) 13 整除 7563257；

(iii) 9、11 整除 742302；(iv) 37 整除 36593。

3. 设 $n=\overline{abc}$ 为三位数。试证：若 $37|n$，则 $37|\overline{bca}$ 且 $37|\overline{cab}$。

4. 试证：$(7\times11\times13)|\overline{abcabc}$，其中 $0<a\leqslant9$，$0\leqslant b$、$c\leqslant9$。

5. 有一五位数形如 $4a77b$ 被 99 整除，试求 a、b。

6. 若 $n\neq0$，$99|n$，那么 $S_1(n)\geqslant18$。

7. 是否存在仅由数码 1 和 0 组成的，其中 1 的个数为 1979 个，0 的个数为 2^{1979} 个，末位数码为 1 且能被 7 整除的整数？

8. 设四位数 $\overline{abca}=(5c+1)^2$，试求该四位数。

9. 试证 n 位数 N，当 $n>1$ 时恒大于它的数码之积。

10. 设一个两位数等于其个位数平方与十位数之和，试求此两位数。

11. 求能被自己的数码之积整除的所有两位数。

12. 把一数的数码按相反顺序排列时为原数的四倍，试给出这种数的最小者。

13. 有一个四位数 $\overline{abcd}$，且 $a+b+c+d=26$，b、d 之积的十位数码等于 $(a+c)$，又 $bd-c^2$ 是 2 的整数次幂，试求此四位数(说明理由)。

14. 试证：对任何大于 5 的 b 进位制中，恒成立着 $1110\times1111\times1112\times1113=(1235431)^2-1$

15. 问：在几进位制中 792 能被 297 整除？

10. 完全平方数

某个整数的平方称为完全平方数，简称平方数。如

$$1,4,9,16,25,36,49,64,81,100,\cdots$$

等等都是平方数。平方数也有许多有趣的性质。例如从上面列出的平方数就可看出：平方数的个位数码只能是 0，1，4，5，6，9 等六个，这是因为平方数 $x=n^2$ 的个位数码是由 n 的个位数码所确定的。有人证明过平方数的末两位数码只能是

00	01	21	41	61	81
	04	24	44	64	84
25	09	29	49	69	89
	16	36	56	76	96

等二十二种。又如在相邻两个整数 n 与 $n+1$ 的平方 n^2 与 $(n+1)^2$ 之间，显然不存在平方数。所以不超过 1000 的正平方数只有 31 个，因为 $31^2=961$，而 $32^2=1024>1000$。

现在，我们将利用上面各节探讨过的整数整除性的性质，通过一些例子来阐述若干与平方数有关的问题。首先讨论由直接分析方法能解的一些例题，然后再讨论一些运用反证法的论证题。先来看与数码有关的平方数的几个问题，它对进一步了解数码特征也是很有帮助的。

【例 1】 若 x 是一个以 5 为末位数码（个位数）的完全平方数，那么它的百位数码必为偶数。

解 设 $x=n^2$，易见 n 的末位数码也是 5。记 $n=10a+5$，其中 a 是某正整数，所以

$$x=n^2=(10a+5)^2=100a(a+1)+25,$$

由于 $2|a(a+1)$，所以百位上的数码是偶数，且只能是 2。

【例 2】 试求一个四位的完全平方数，若已知它的前两数码相同，后两数码也相同。

解 记这一个四位数为 $\overline{aabb}$，因为

$$\begin{aligned}\overline{aabb} &= a\times 10^3 + a\times 10^2 + b\times 10 + b\\ &= (a\times 10^2 + b)\times 11 = \overline{a0b}\times 11,\end{aligned}$$

所以欲使它是完全平方数，三位数 $\overline{a0b}$ 必须含素因数 11。由 §9 性质 22系 2 可知，$11|\overline{a0b}$ 当且仅当 $11|(a+b)$。注意到 a、b 是 $0,1,\cdots,9$ 诸数码之一 $(a\neq 0)$，故共有 $(2,9),(3,8),(4,7),\cdots,(9,2)$ 等 8 组可能值。直接验算，可知只当 $a=7$，$b=4$ 时，$\overline{a0b}=704=8^2\times 11$ 满足要求，此时所求的四位数为 $7744=88^2$。

【例 3】 一个两位数 N，在它的左边添上适当的两个数码变成四位数时恰是原数 N 的平方，试求所有这样的两位数。

解 设添上的二个数码为 a、b，记 $k=\overline{ab}$。按题意有

$$k\times 100 + N = N^2 \text{ 即 } N(N-1) = 2^2 5^2 k。$$

欲使 N^2 是一个四位数，必须 $N\geqslant 32$。又 N 与 $N-1$ 互素，所以由 $2^2 5^2|N(N-1)$ 可得：或者 $2^2|N$，$5^2|(N-1)$；或者 $5^2|N$，$2^2|(N-1)$。

当 $5^2|N$，$2^2|(N-1)$ 时，N 必为奇数。这就是说 N 必是大于 32 且为 $5^2=25$ 的倍数的奇两位数，这样的两位数 N 可能取的值只有 75，但此时 $2^2\nmid 74$，所以此时无解。

同理，当 $2^2|N$，$5^2|(N-1)$ 时，这时 $N-1$ 可能取的值只有 75，此时 $2^2|76$，所以 $N=76$。

这就解得只有 76 这一个两位数满足所说性质：$5776=76^2$。

【例 4】 求具有下列性质的最大的平方数：在抹去它的个位数码和十位数码后仍为完全平方数（被抹去的两位数不

全为 0)。

解 设把 n^2 中后两位数码抹去后得 k^2，且 n^2 不是以 00 结尾的，所以有

$$0 < n^2 - 100k^2 < 100 \tag{1}$$

由 $0 < n^2 - 100k^2$ 得 $n > 10k$，即 $n \geqslant 10k + 1$，由此

$$100 > n^2 - 100k^2 \geqslant (10k + 1)^2 - 100k^2 = 20k + 1,$$

所以 $k \leqslant 4$。当 $k = 4$ 时，因为 $42^2 - 100 \times 4^2 > 100$，即 $n = 42$ 不满足 (1) 式，故欲 (1) 的右边不等式成立只有 $n=41$。直接验证知 $n^2 = 41^2 = 1681$ 是满足所述性质的数。从上述的证明可见，由于 k 要满足 (1) 式，除 41^2 外已无更大的数满足所述性质。

下面讨论几个用直接分析的方法能解的例题。

【例 5】 试证和数

$$\overbrace{11\cdots1}^{m} \times \overbrace{10\cdots05}^{m+1} + 1$$

是完全平方数。

证 容易看出

$$\begin{aligned}&\overbrace{11\cdots1}^{m} \times \overbrace{10\cdots05}^{m+1} + 1\\ &= \frac{1}{9}(10^m - 1)(10^m + 5) + 1\\ &= \frac{1}{9}(10^m + 2)^2 = \left(\frac{10^m + 2}{3}\right)^2。\end{aligned}$$

易知 $3|(10^m + 2)$，故得证所给和数是平方数。

【例 6】 试求能使 $22n + 5$ 为完全平方数的一切自然数 n，并给出这种 n 的一般表示式。

解 设 $22n + 5 = N^2$，其中 N 是自然数。于是

$$N^2 - 16 = 11(2n - 1),$$

由此可得，或者 $N - 4$ 或者 $N + 4$ 是 11 的倍数。但由于 N 是奇数，所以 $N = (2k - 1) \times 11 \pm 4$，即

$$N = 22k - 7 \text{ 或 } N = 22k - 15 \quad (k = 1, 2, \cdots)。$$

因此解得：

$$n = \frac{1}{22}(N^2 - 5) = \frac{1}{22}[(22k - 7)^2 - 5]$$

$$= 22k^2 - 14k + 2 \quad (k = 1, 2, \cdots)$$

或

$$n = \frac{1}{22}(N^2 - 5) = \frac{1}{22}[(22k - 15)^2 - 5]$$

$$= 22k^2 - 30k + 10 \quad (k = 1, 2, \cdots)。$$

【例 7】 是否存在两个自然数 a、b，使得 $a^2 + 2b$ 和 $b^2 + 2a$ 同时都是完全平方数？

解 回答是否定的。在 $a \geqslant b > 0$ 的情况下，由

$$a^2 < a^2 + 2b \leqslant a^2 + 2a < (a + 1)^2$$

可知，$a^2 + 2b$ 不可能是完全平方数。同理，在 $b \geqslant a > 0$ 的情况下，$b^2 + 2a$ 也不可能是完全平方数。所以不论 a、b 是怎样的自然数，$a^2 + 2b$ 和 $b^2 + 2a$ 不能同时都是完全平方数。注意：两者之中有一个为完全平方数是可能的，如 $a = 3$，$b = 20$，$a^2 + 2b = 49$ 就是完全平方数。

下面给出运用反证法论证的几个例题。反证法是大家熟悉的一种逻辑演绎法，前几节也曾多次用到，不少问题直接证很困难，甚至无从证起，往往一用反证法，问题便比较容易解了。

【例 8】 用 300 个 2 和若干个 0 写出的整数会不会是一个完全平方数？

解 不会。用反证法。记依题意写出的整数为 a，其数码和 $S_1(a) = 300 \times 2 = 600$，故 $3 | S_1(a)$，由此 $3 | a$，并进而有 $9 | a$ 及 $9 | 600 = S_1(a)$。但这是不可能的，由此得证 a 不会是完全平方数。

【例 9】 证明：相继三个自然数中的最大一数的立方不

能等于另两个数的立方和。

证 设相继三数为 $n-1, n, n+1$，若有 $(n+1)^3=n^3+(n-1)^3$，便可得 $2=n^2(n-6)$，由此必有 $n>6$。但此时右边 $n^2(n-6)>36>2$，即 $n^2(n-6)\neq 2$，矛盾。

【例 10】 设 n 是自然数，$2n^2$ 被自然数 d 整除，试证 n^2+d 不是平方数。

证 由假设 $2n^2=kd$。若 $n^2+d=a^2$，那么由 $2n^2=kd$ 得：

$$2n^2+n^2k=kd+n^2k,$$

即 $n^2(k+2)=k(n^2+d)$，于是

$$(k+2)/k=(n^2+d)/n^2=a^2/n^2。$$

上式左边分子、分母相差为2，当约去其公因数后，这个差只会减小，右边分式在约去公因数后可写成 p^2/q^2，其中 p、q 都是自然数且 $p>q$，故 $p-q\geqslant 1$，$p+q\geqslant 3$，所以分式 p^2/q^2 的分子和分母的差 $p^2-q^2\geqslant 3$，矛盾。

习 题 10

1. 试证对任何正整数 n，数 $n^4+2n^3+2n^2+2n+1$ 不会是完全平方数。

2. 试求有多少个四位数，它加上 400 后就成为一个自然数的完全平方。

3. 试问数 11111 在什么进位制中恰好表示一个平方数？

4. 试求四位的完全平方数，它的千位数是其十位数加8，它的百位数是其个位数减 4。

5. 求出所有满足下列条件的两位数：它比用它的两个

数码倒排后所得的数大一个完全平方数。

6. 有一正整数，若加上 200 为一个完全平方数，若加上 292 为另一个完全平方数，试求这一正整数。

7. 证明五个相继正整数的平方和不是完全平方数。

8. 在一个 100 位数 N 中，除其中一个外其余所有数码都是 5，证明它不是完全平方数。

9. 设三个整数 a,b,c 没有异于 1 的公因数，且

$$\frac{1}{a}+\frac{1}{b}=\frac{1}{c},$$

试证 $a+b$，$a-c$ 和 $b-c$ 都是平方数。

10. 证明对任何自然数 m，数 $m(m+1)$ 不可能是某一整数的方幂。[提示：注意 m 与 $m+1$ 互素。]

11. 整数数列中的一些问题

按一定顺序排列的数 $u_0, u_1, u_2, \cdots, u_n, \cdots$ 称为数列，简记作 $\{u_n\}$。若数列中的每一项都是整数，就称这样的数列为整数数列。比方说：

奇数数列 $1,3,5,7,\cdots,2n+1,\cdots$

等差数列 $3,7,11,15,\cdots,4n+3,\cdots$

平方数数列 $1,4,9,16,\cdots,n^2,\cdots$

素数数列 $2,3,5,7,11,\cdots,p_n,\cdots$

等都是整数数列。在§8例4中我们已讨论过上面 $4n+3$ 型等差数列中有无穷多个素数。对于一般情形，已有人证明，若 a、b 互素，那么等差数列 $\{an+b\}$ 中也有无穷多个素数。整数数列还有许多十分引人入胜的问题，如以某些素数组成的等差数列中就有一些颇饶兴趣的与整除有关联的性质，又如闻名的兔子数列(也称斐波那契数列)性质和谐，至今还在某些数学分支中有应用。

在这一节里我们将综合运用前面各节的知识，通过例子来介绍某些整数数列及其性质。先看几个关于等比数列及素数组成的等差数列的简单例子。

【例 1】 若三个大于 10 的素数成等差数列，其公差为 d，那么 $6|d$。

证 设此三个素数为 p_1, p_2, p_3。因大于 10 的素数都是奇数，所以其差必为偶数，即 $2|d$。余下只要证 $3|d$。若不然，$3\nmid d$。当 $d=3k+1$ 时，若 $p_1=3l+1$，那么 $p_3=p_1+2d=3(2k+l+1)$ 不是素数，与 p_3 是素数的假设矛盾；若

$p_1=3l+2$，那么 $p_2=p_1+d=3(k+l+1)$ 也不是素数，与 p_2 是素数的假设矛盾。

同理，当 $d=3k+2$ 时，若 $p_1=3l+1$，那么 $p_2=p_1+d=3(k+l+1)$ 不是素数；若 $p_1=3l+2$，那么 $p_3=p_1+2d=3(2k+l+1)$ 也不是素数，与假设矛盾。这就得证 $2|d$ 且 $3|d$，所以 $6|d$。

例 1 所证明的性质在后面还要用到。

【例 2】 证明等比数列

$$1, 10^4, 10^8, \cdots, 10^{4n}, \cdots$$

的前 n 项的和 S_n，当 $n\geqslant 2$ 时都是合数。

证 原等比数列的前 $n+1$ 项之和记为 S_{n+1}，即

$$S_{n+1}=1+10^4+10^8+\cdots+10^{4n}。$$

记 $b_{n+1}=1+10^2+10^4+\cdots+10^{2n}$ $(n=1,2,\cdots)$。因为

$$10^{4n+4}-1=(10^4-1)(1+10^4+\cdots+10^{4n})$$
$$=(10^4-1)S_{n+1},$$
$$10^{2n+2}-1=(10^2-1)(1+10^2+\cdots+10^{2n})$$
$$=(10^2-1)b_{n+1},$$

所以由 $10^{4n+4}-1=(10^{2n+2}-1)(10^{2n+2}+1)$ 得

$$101\times S_{n+1}=b_{n+1}(10^{2n+2}+1)=b_{n+1}[(10^2)^{n+1}+1]$$

即：
$$S_{n+1}=b_{n+1}\frac{(10^2)^{n+1}+1}{101}。$$

当 $n=1$ 时，直接计算知 $S_2=10001=73\times 137$ 是合数；当 n 是正偶数时，$101|[(10^2)^{n+1}+1]$，故 S_{n+1} 也是合数。

当 n 是大于 2 的奇数时，写 $n=2k+1$ $(k=1,2,\cdots)$，有

$$b_{n+1}=(10^2+1)(1+10^4+\cdots+10^{4k})=101\times S_{k+1},$$

此时 $S_{n+1}=S_{k+1}\times(10^{2n+2}+1)$ 也是合数。证毕。

【例 3】 已知由正整数组成的等比数列

$$7,\quad 28,\quad 112,\quad 448,\cdots,\ 7\cdot 4^n,\cdots$$

$$15,\quad 60,\quad 240,\quad 960,\cdots,15\cdot 4^n,\cdots$$

$$23,\quad 92,\quad 368,\quad 1472,\cdots,23\cdot 4^n,\cdots$$

$$31,\quad 124,\quad 496,\quad 1984,\cdots,31\cdot 4^n,\cdots。$$

试证：这些数列中的任何一项都不是完全平方数，也不是两个或三个平方数的和。

解 首先注意到这四个等比数列的一般项为 $4^n(8k-1)$，$k=1,2,3,4$。用反证法，若有

$$4^n(8k-1)=x^2+y^2+z^2, \tag{1}$$

其中 x,y,z 是非负整数。

当 $n>0$ 时，x,y,z 必须都是偶数，事实上，若此三数中有奇数，因(1)式左边为偶数，由奇偶性可知，此时 x,y,z 中不可能只有一个或三个都是奇数（否则右边的和就成为奇数，矛盾）。即只可能两个为奇数，一个为偶数。不妨设 x,y 为奇数，记 $x=2a+1$，$y=2b+1$；z 为偶数，记 $z=2c$。此时(1)式右边

$$\begin{aligned}x^2+y^2+z^2&=(2a+1)^2+(2b+1)^2+(2c)^2\\&=4(a^2+a+b^2+b+c^2)+2,\end{aligned}$$

它不是 4 的倍数，这与左边 $4^n(8k-1)$ 当 $n>0$ 时是 4 的倍数相违。从而证明了 x、y、z 必须同时为偶数。记

$$x=2x_1,\quad y=2y_1,\quad z=2z_1,$$

代入(1)式得

$$4^{n-1}(8k-1)=x_1^2+y_1^2+z_1^2。$$

同样讨论，若 $n>1$，那么 x_1、y_1、z_1 也必须都是偶数。由此又可得等式

$$4^{n-2}(8k-1)=x_2^2+y_2^2+z_2^2,$$

不断进行这样的手续，最后得 $8k-1$ 也能表为三个非负整数的平方和

$$8k-1=X^2+Y^2+Z^2。$$

此时左边为奇数，那么X、Y、Z只能有一个或三个都是奇数。但奇数$2l+1$的平方$(2l+1)^2=4l(l+1)+1$被8除余数恒为1。偶数m平方被8除的余数为0（若$4|m$）或余数为4（若$4\nmid m$）。这样当X、Y、Z都为奇数的情形下，$X^2+Y^2+Z^2=8M+3$；当X、Y、Z中只有一个为奇数情形下，$X^2+Y^2+Z^2=8M+1$或$8M+5$。因此，在上述任何一种情形下，三整数的平方和不可能为$8k+7=8(k+1)-1$型，亦即$8k-1$不可能表成三个非负整数的平方和。这就用反证法证得命题成立。

下面讨论有着悠久历史的兔子数列。早在公元1202年有个绰号叫斐波那契（Fibonacci）的意大利人从兔子的繁殖问题提出一个数列，后人也称这个数列为斐波那契数列。然而，因为流传着离奇的兔子的故事，人们还是常称它为兔子数列。故事的梗概是这样：假定每对大兔子每月都能生一对（一公、一母）小兔子，小兔子一个月后即长成为大兔子，再过一个月后又会生一对小兔子。现在某人年初买进一对小兔子，问到年底时他共有几对兔子？下面的表格给出了这个问题的解。

月份	0	1	2	3	4	5	6	7	8	9	10	11	12
小兔对数	0	1	0	1	1	2	3	5	8	13	21	34	55
大兔对数	0	0	1	1	2	3	5	8	13	21	34	55	89
总对数	0	1	1	2	3	5	8	13	21	34	55	89	144

表中最后一行就是兔子数列。它的递推公式是

$$u_0=0,\ u_1=u_2=1,\ u_{n+1}=u_n+u_{n-1}(n\geqslant 2)。$$

【例4】 试证：兔子数列中任意相邻的两个兔子数都是

互素的，即 $(u_{n+1}, u_n) = 1 \quad (n \geqslant 1)$。

证 记 $(u_{n+1}, u_n) = d$。由性质 5，$(b+c, b) = (b, c)$，所以有

$$
\begin{aligned}
d &= (u_{n+1}, u_n) = (u_n + u_{n-1}, u_n) \\
&= (u_n, u_{n-1}) = (u_{n-1} + u_{n-2}, u_{n-1}) \\
&= (u_{n-1}, u_{n-2})。
\end{aligned}
$$

依此类推得证

$$
\begin{aligned}
d &= (u_{n+1}, u_n) = (u_n, u_{n-1}) = (u_{n-1}, u_{n-2}) \\
&= \cdots = (u_3, u_2) = (u_2, u_1) \\
&= (1, 1) = 1。
\end{aligned}
$$

【例 5】 试证在兔子数列中，当 $4 \mid n$ 时就有 $3 \mid u_n$。

证 用数学归纳法。由假设 $4 \mid n$，即 $n = 4k$。当 $k=1$ 时，$u_4 = 3$，即 $k=1$ 时命题成立。归纳假设当 $k=l$ 时命题成立，即 $u_{4l} = 3m$。在 $k = l+1$ 时，由于

$$
\begin{aligned}
u_{4l+1} &= u_{4l} + u_{4l-1}, \\
u_{4l+2} &= u_{4l+1} + u_{4l} = 2u_{4l} + u_{4l-1}, \\
u_{4l+3} &= u_{4l+2} + u_{4l+1} = 3u_{4l} + 2u_{4l-1}, \\
u_{4(l+1)} &= u_{4l+3} + u_{4l+2} = 5u_{4l} + 3u_{4l-1} \\
&= 3(5m + u_{4l-1})。
\end{aligned}
$$

得证当 $k = l+1$ 时，$u_{4(l+1)}$ 也是 3 的倍数，由是对每一自然数 k，u_{4k} 是 3 的倍数。

【例 6】 在兔子数列 $\{u_n\}$ 的前 100000001 项中是否存在一个末四位数码都为 0 的兔子数？

证 实质上，问题可以归结为研究兔子数列 $\{u_n\}$ 中每一项的末四位数码的结构，换句话说，不管 u_n 是五位或更多位数，仅需讨论去掉第四位以前的诸数码后所留下的四个数码所构成的数，亦即小于 10^4 的部分(如 347352，去掉 34，留下 7352)，记此数为 a_n。若已知 a_{k+1} 与 a_k，那么便可求得 a_{k-1}，

这是因为 $u_{k+1}=u_k+u_{k-1}$，所以 $a_{k+1}=a_k+a_{k-1}$ 或 $a_{k+1}=a_k+a_{k-1}-10000$。

现在，若能证明存在某两自然数 k，n 使得 $a_k=a_{n+k}$，且 $a_{k+1}=a_{n+k+1}$，那么由上述关系就有

$$a_{k-1}=a_{n+k-1},\ a_{k-2}=a_{n+k-2},\cdots,\ a_1=a_{n+1},a_0=a_n。$$

因 $a_0=0$，则必有 $a_n=0$，这意味着兔子数列的第 $n+1$ 项 u_n 是四个 0 结尾的数。

综上所述只要证明：存在两自然数 k，n 使得 $a_k=a_{n+k}$，$a_{k+1}=a_{n+k+1}$。注意到，在

$$(a_0,a_1),\ (a_1,a_2),\ (a_2,a_3),\cdots,(a_{10^8},a_{10^8+1})$$

等 10^8+1 个数对中，由于 $a_0,a_1,\cdots,a_{10^8}$ 每一数都不大于 10^4，即都是 $0,1,2,\cdots,9999$ 诸数之一，所以 (a_i,a_{i+1}) 的一切可能情形至多有 $10^4\times10^4=10^8$ 种。因此，在上述 10^8+1 个数对中必有两个数对相同，这就是说 $(a_k,a_{k+1})=(a_{k+n},a_{k+n+1})$，即得证有 k，n 使 $a_k=a_{k+n}$，$a_{k+1}=a_{k+n+1}$。证毕。

具体讨论后可知 u_{7500} 是末四位数码为 0 的兔子数。

关于兔子数列的另几个简单性质放在习题中，请读者自己证明。最后我们讨论由素数与平方数组成的数列的几个例子。

【例 7】 试证三个不同素数的立方根不可能作为一个等差数列中的某三项(不必相邻)。

证 用反证法。若不然，设有三个素数 $p>q>r$（或 $p<q<r$），它们的立方根 $\sqrt[3]{p},\sqrt[3]{q},\sqrt[3]{r}$ 是某等差数列中的三项。如该等差数列的公差为 d，那么有

$$\sqrt[3]{p}=\sqrt[3]{q}-md,\ \ \sqrt[3]{q}=\sqrt[3]{r}-nd。$$

其中 m、n 为两个自然数。消去 d 得

$$(m+n)\sqrt[3]{q}=n\sqrt[3]{p}+m\sqrt[3]{r},$$

两边立方后，并利用原关系式得

$$(m+n)^3q=n^3p+m^3r+3mn\sqrt[3]{pr}\times(n\sqrt[3]{p}+m\sqrt[3]{r})$$
$$=n^3p+m^3r+3mn(m+n)\sqrt[3]{pqr},$$

即

$$\sqrt[3]{pqr}=\frac{(m+n)^3q-n^3p-m^3r}{3mn(m+n)}。$$

上式右边是有理数，因 p, q, r 是不同的素数，左边是无理数，矛盾。因此三个不同素数的立方根，不能是一个等差数列中的三项。

【例 8】 试找出六个小于 160 而成等差数列的素数。证明不可能有七个皆小于 200 的素数成等差数列。

解 例 1 已证，此时等差数列的公差 d 是 6 的倍数。现在来证 $5|d$。用反证法。若不然 $5\nmid d$，注意到整数 a, $a+d$, $a+2d$, $a+3d$, $a+4d$，在 $5\nmid d$ 时，这五个数被 5 除时所得余数必各不相同，(因若有 $a+id$ 与 $a+jd$ 被 5 除时余数相同，那么 $5|((a+id)-(a+jd))$，即 $5|(i-j)d$，由于 $0<|i-j|<5$，故 $5\nmid(i-j)$，因此必 $5|d$，这与已设 $5\nmid d$ 相违。)这样，这六个素数任意相继的五个中就有一个是 5 的倍数，即使 $p_1=5$，那么素数 p_2, p_3, p_4, p_5, p_6 中也有一个是 5 的倍数，这与素数的假定矛盾。因此得证 $5|d$。

由 $5|d$, $6|d$，且 $(5,6)=1$，所以 $30|d$, $d=30k$，按题设得 $k=1$, $d=30$，$p_1+150<160$，所以 $p_1<10$。此时 p_1 可能值只有 3,5,7。易见 $p_1=3,5$ 时，$p_1+30=33,35$ 都不是素数，不合。仅当 $p_1=7$ 时，

$$7,37,67,97,127,157$$

六个素数成等差数列。

若有七个小于 200 的素数成等差，那么

$$p_7 = p_1 + 6d = p_1 + 180k < 200,$$

所以 $k = 1$, $d = 30$, $p_1 < 20$。此时 p_1 的可能值只有 3, 5, 7, 11, 13, 17, 19。直接验证知 $p_1 = 3, 5, 19$ 时，$p_1 + d = 33$, 35, 49 均为合数，$p_1 = 17$ 时，$p_1 + 2d = 77 = 7 \times 11$; $p_1 = 13$ 时，$p_1 + 4d = 133 = 7 \times 19$; $p_1 = 11$ 时，$p_1 + 5d = 161 = 7 \times 23$; $p_1 = 7$ 时，$p_1 + 6d = 187 = 17 \times 11$ 均为合数。所以无小于 200 的七个素数成等差数列。

【例 9】 若有 14 个不同的素数能成为等差数列相继的 14 项，那么该数列的公差 d 大于 30000。

证 在例 1 和例 8 中已证 $2 \times 3 \times 5 | d$。我们来证此时公差 d 能被 2, 3, 5, 7, 11, 13 整除。如以 13 为例，考察这 14 个素数被 13 除时的余数。首先，没有一个余数为 0。若不然，如 $13 | p_1$，那么素数 $p_1 = 13$，但此时 $p_{14} = p_1 + 13d = 13 \times (d + 1)$ 为合数，与 p_{14} 是素数的假设矛盾。若 $13 | (p_1 + id)$，$(0 < i \leqslant 13)$，则 $p_{i+1} = p_1 + id = 13$。由已知 $d = 30k$，$(k \geqslant 1)$，所以不存在这样的素数 p_1，使 $p_{i+1} = 13 = p_1 + id = p_1 + 30ik$。因此，除去 p_1 与 $p_{14} = p_1 + 13d$ 除以 13 时余数相同外，必有 $p_1 + id$ 与 $p_1 + jd$ $(i \neq j, 0 \leqslant i, j \leqslant 13)$ 除以 13 时余数相同，这样 $13 | (i - j)d$，从而 $13 | d$。

同理可证 7, 11 也能整除 d，所以

$$d \geqslant 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030。$$

【例 10】 已知数列

$$a_1 = 1, a_2 = a_1 + [\sqrt{a_1}], a_{n+1} = a_n + [\sqrt{a_n}], \quad n = 1, 2, \cdots。$$

试证：当且仅当 $n = 2^k + k - 2$ (k 为正整数)时，a_n 是平方数。这里，记号 $[x]$ 表示不超过 x 的最大整数。

证 对 k 用数学归纳法证明：当 $n = n_k = 2^k + k - 2$

时，$a_n=(2^{k-1})^2$，当 $n_{k-1}<m<n_k$ 时，a_m 不是完全平方数。

当 $k=1$ 时，$n_1=1$，$a_{n_1}=a_1=1$ 是平方数，且为 $(2^{1-1})^2$，即命题对 $k=1$ 成立。设命题对某 k 成立，即 $n_k=2^k+k-2$ 时，$a_{n_k}=(2^{k-1})^2$。

现在记 $n=n_k$。我们先用归纳法来证，当 $n_k<m<n_{k+1}$ 时有

$$a_{n+2i+1}=(2^{k-1}+i)^2+2^{k-1}-i,\quad 0\leqslant i\leqslant 2^{k-1},\qquad (2)$$

$$a_{n+2i}=(2^{k-1}+i-1)^2+2^k,\qquad 1\leqslant i\leqslant 2^{k-1}。\qquad (3)$$

事实上，当 $i=0$ 时，(2)式中

$$\text{左边}=a_{n+1}=a_n+[\sqrt{a_n}]=(2^{k-1})^2+2^{k-1}=\text{右边},$$

当 $i=1$ 时，(3)式中

$$\begin{aligned}\text{左边}&=a_{n+2}=a_{n+1}+[\sqrt{a_{n+1}}]\\&=(2^{k-1})^2+2^{k-1}+[\sqrt{(2^{k-1})^2+2^{k-1}}]\\&=(2^{k-1})^2+2^{k-1}+2^{k-1}\\&=(2^{k-1})^2+2^k=\text{右边}。\end{aligned}$$

现在归纳假设 $i<l(<2^{k-1})$ 时 (2)、(3) 成立，当 $i=l$ 时，(2)式中

$$\begin{aligned}\text{左边}&=a_{n+2l+1}=a_{n+2l}+[\sqrt{a_{n+2l}}]\\&=(2^{k-1}+l-1)^2+2^k\\&\quad+[\sqrt{(2^{k-1}+l-1)^2+2^k}]\\&=(2^{k-1}+l-1)^2+2^k+2^{k-1}+l-1\\&=(2^{k-1}+l)^2+2^{k-1}-l=\text{右边}。\end{aligned}$$

当 $i=l$ 时，(3) 式中

$$\begin{aligned}\text{左边}&=a_{n+2(l+1)}=a_{n+2l+1}+[\sqrt{a_{n+2l+1}}]\\&=(2^{k-1}+l)^2+2^{k-1}-l\\&\quad+[\sqrt{(2^{k-1}+l)^2+2^{k+1}-l}]\\&=(2^{k-1}+l)^2+2^{k-1}-l+2^{k-1}+l\\&=(2^{k-1}+l)^2+2^k=\text{右边}。\end{aligned}$$

而当(2)中 $i=2^{k-1}$ 时，$n+2i+1=n_k+2^k+1=2^k+k-2+2^k+1=2^{k+1}+(k+1)-2=n_{k+1}$。由(2)即得

$$a_{n_{k+1}}=(2^{k-1}+2^{k-1})^2+2^{k-1}-2^{k-1}=(2^k)^2。$$

这样由(2)和(3)就证明了当 $k+1$ 时 $a_{n_{k+1}}=(2^k)^2$，且由(2),(3)可知，当 $n_k<m<n_{k+1}$（即(2)中 $i<2^{k-1}$ 时,(3)中 $i\leqslant 2^{k-1}$ 时），$a_m=a_{n+2i+1}$ 或 a_{2n+i} 都不是平方数。这就得证命题对一切自然数 k 成立。

习　题　11

1. 设前 n 个偶数的立方和与前 n 个奇数的立方和之差为 2240，试求 n。

2. 试证不可能由不同的素数组成一个无穷等差数列。

3. 试求三个自然数 a，b，c，使其两两之积成等差数列。

4. 证明若 $a, a+d, a+2d, \cdots, a+(n-1)d$ 与 n 互素，那么 $(d,n)>1$。

5. 已知相继若干个自然数之和为 1000，试求出所有这种数列。

6. 试证在兔子数列 $\{u_n\}$ 中：

(i) 当 $5|n$ 时，则 $5|u_n$，

(ii) 当 $6|n$ 时，则 $4|u_n$。

7. 设素数 p_1，p_2，p_3 是公差为 d 的等差数列中相继的三项。证明若 $6\nmid d$，那么 $p_1=3$，且这样的数组唯一，试给出 $d\leqslant 20$ 的那些素数组。

8. 设数列

$\{x_n\}$：$x_0=0$，$x_1=1$，$x_{n+1}=x_n+2x_{n-1}$，

$\{y_n\}$：$y_0=1$，$y_1=7$，$y_{n+1}=2y_n+3y_{n-1}$，

即 $\{x_n\}$: 1,1,3,5,11,21,···;$\{y_n\}$:1,7,13,55,161,487,···除去1外,在两数列中没有相同的数。

9. 试找出十个小于3000而成等差数列的素数。

12. 同　余

1979 年 5 月 20 日我国第一次举行全国性的中学数学竞赛，同年 7 月 28 日发奖。已知 1979 年 1 月 1 日是星期 1，试问竞赛和发奖那天分别是星期几？这种问题在日常生活中是经常出现的。我们不妨来试解这个问题。由于每星期有 7 天，1979 年元旦是星期一，那么计算出 1 月 1 日至 5 月 20 日共有 140 天，它被 7 除的余数是 0，可知 1979 年 5 月 20 日是星期日。同理，1 月 1 日至 7 月 28 日共有 209 天，它被 7 除的余数是 6（$209=7\times 28+6$），所以 1979 年 7 月 28 日发奖恰是星期 6。这种对于整数除以某一确定的整数时，只关心余数的情况，在数学上产生所谓"同余"的概念。一般地，有

定义　对于固定的正整数 m，若用 m 去除给定的整数 a 与 b 所得的余数相同，就称整数 a 与 b 对于模 m 同余，记作 $a\equiv b \pmod{m}$。

反之，称 a 与 b 对于模 m 不同余，记作 $a\not\equiv b \pmod{m}$。

【例 1】　下列诸数哪一些对于模 7 互相同余：

$$356,\ 44,\ 85,\ -5,\ 36,\ 6。$$

解　由 $356=7\times 50+6$，所以 $356\equiv 6 \pmod{7}$；

$44=7\times 6+2$，$-5=7\times(-1)+2$，所以 $44\equiv -5 \pmod{7}$；

$85=7\times 12+1$，$36=7\times 5+1$，所以 $85\equiv 36 \pmod{7}$。

很明显，同余概念与整除性是有十分密切的关系的。

性质 23　(i) $a\equiv b \pmod{m}$ 当且仅当 $m\mid(a-b)$。

(ii) 若 $a\equiv b \pmod{m}$，$l\mid m$，则 $a\equiv b \pmod{l}$。

证　(i) 设 $a\equiv b \pmod{m}$，即 $a=mq+r$，$b=mq_1+r$，

$0 \leqslant r < m$，q、q_1 为整数，那么 $a - b = m(q - q_1)$，即得 $m|(a-b)$。

反之，当 $m|(a-b)$ 时，$a - b = mk$，k 为整数。若 $b = mq_1 + r$，那么代入即得 $a = b + mk = m(q_1 + k) + r$，因此，$a \equiv b \pmod{m}$。

(ii) 由 (i) 知 $m|(a-b)$，故若 $l|m$，那么就有 $l|(a-b)$，再由 (i) 推出 $a \equiv b \pmod{l}$。

同余还有下述明显的基本性质。

性质 24 (i) $a \equiv a \pmod{m}$（反射性）;

(ii) 若 $a \equiv b \pmod{m}$，那么 $b \equiv a \pmod{m}$（对称性）;

(iii) 若 $a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$ 那么 $a \equiv c \pmod{m}$（传递性）。

应用性质23及整除性的基本性质还可导出下述同余的基本运算法则。

性质 25 (i) 若 $a_1 \equiv b_1 \pmod{m}$，$a_2 \equiv b_2 \pmod{m}$，那么 $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$，$a_1a_2 \equiv b_1b_2 \pmod{m}$;
特别，如 $a + b \equiv c \pmod{m}$，则 $a \equiv c - b \pmod{m}$;

如 $a \equiv b \pmod{m}$，则 $a^l \equiv b^l \pmod{m}$，$ka \equiv kb \pmod{m}$，（k 为整数，l 为正整数）。

(ii) 若 $a = a_1d$，$b = b_1d$，$a \equiv b \pmod{m}$ 且 $(d, m) = 1$，那么 $a_1 \equiv b_1 \pmod{m}$。

(iii) 若 $a_i \equiv b_i \pmod{m}$，$i = 0, 1, \cdots, n$，那么对任何整数 x，

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$$
$$\equiv b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0 \pmod{m}。$$

证 (i) 由性质 23，此时 $m|(a_1 - b_1)$，$m|(a_2 - b_2)$，所以由性质 2，$m|[(a_1 - b_1) \pm (a_2 - b_2)]$，即 $m|[(a_1 \pm a_2) - (b_1 \pm b_2)]$，再由性质 23 即得。

注意到 $m \mid (a_1 - b_1)(a_2 - b_2)$, $m \mid b_1(a_2 - b_2)$, $m \mid b_2 \times (a_1 - b_1)$; 以及有

$$a_1a_2 - b_1b_2 = (a_1 - b_1)(a_2 - b_2) + b_1(a_2 - b_2) + b_2(a_1 - b_1),$$

故由性质 2, m 能整除上式右边，从而 $m \mid (a_1a_2 - b_1b_2)$, 应用性质 23, 得 $a_1a_2 \equiv b_1b_2 (\mathrm{mod}\ m)$。

特别，由 $-b \equiv -b(\mathrm{mod}\ m)$, 若 $a + b \equiv c(\mathrm{mod}\ m)$, 则 $a + b + (-b) \equiv c + (-b)(\mathrm{mod}\ m)$ 即 $a \equiv c - b(\mathrm{mod}\ m)$。当 $a_1 = a_2$, $b_1 = b_2$ 时，就有 $a^2 \equiv b^2(\mathrm{mod}\ m)$, 一般地有 $a^l \equiv b^l(\mathrm{mod}\ m)$, $ka \equiv kb(\mathrm{mod}\ m)$。

(ii) 依条件及按性质 23, $m \mid (a-b)$, 则有 $m \mid (a_1 - b_1)d$, 而 $(d, m) = 1$, 故由性质 9, 即得 $m \mid (a_1 - b_1)$, 再利用性质 23, 便是 $a_1 \equiv b_1(\mathrm{mod}\ m)$。

(iii) 因 $a_i \equiv b_i(\mathrm{mod}\ m)$, $x^i \equiv x^i(\mathrm{mod}\ m)$, 故由 (i),

$$a_ix^i \equiv b_ix^i(\mathrm{mod}\ m) \quad (i = 0, 1, \cdots, n)。$$

再由 (i) 得

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \equiv b_nx^n + b_{n-1}x^{n-1} + \cdots + b_0 \ (\mathrm{mod}\ m)。$$

下面我们用同余的特征，解某些有关整除性的问题。

【例 2】 设整数 $N = \overline{a_na_{n-1}\cdots a_1a_0}$, 试用同余性质，证明：$9 \mid N$ 的充要条件是 $9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$。

解 由于 $a_i10^i = a_i \times \overbrace{9\cdots9}^{i-1}9 + a_i$, 即 $a_i10^i \equiv a_i(\mathrm{mod}\ 9)$, 所以，由性质 25 (i),

$$N = \overline{a_na_{n-1}\cdots a_1a_0} = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0$$
$$\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 (\mathrm{mod}\ 9),$$

按定义，即有 $9 \mid N$ 当且仅当 $9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$。

【例 3】 若整数 a、b、c 为完全平方数，且 $9|(a+b+c)$，那么在 a、b、c 中至少有两数，其差能被 9 整除。

解 注意到任一整数 $x=9k+r$，$r=0,1,\cdots,8$。

当 $r=0,3,6$ 时，$x^2\equiv r^2\equiv 0(\bmod 9)$，

当 $r=1,8$ 时，$x^2\equiv r^2\equiv 1(\bmod 9)$，

当 $r=2,7$ 时，$x^2\equiv r^2\equiv 4(\bmod 9)$，

当 $r=4,5$ 时，$x^2\equiv r^2\equiv 7(\bmod 9)$。

所以若 a、b、c 为完全平方数且 $9|a+b+c$，那么 a、b、c 对于模 9 或均与 0、0、0 同余，或分别与 1、4、4 同余，或分别与 1、1、7 同余。不论哪一种情形，由性质 24，a、b、c 三数中至少有两数对于模 9 同余，即其差能被 9 整除。

从上面两个例子看到，利用同余解某些整除问题，条理清晰，叙述简明。现在再来讨论关于同余的两个例子。

【例 4】 设 $n_1, n_2, \cdots, n_k$ 是 k 个正整数，记前 i 个数的最大公因数为 $(n_1, n_2, \cdots, n_i)$，令 $d_1=1$，

$$d_i=\frac{(n_1,n_2,\cdots,n_{i-1})}{(n_1,n_2,\cdots,n_i)}\quad(i=2,\cdots,k)。$$

试证当每一个 a_i 取遍 $1,2,\cdots,d_i$ 时，在 $d_1d_2\cdots d_k$ 个可能的和数 $a_1n_1+a_2n_2+\cdots+a_kn_k$ 中，任两个对于模 n_1 互不同余。

证 用反证法。若不然，设

$$\begin{aligned}&a_1n_1+a_2n_2+\cdots+a_kn_k\\&\equiv b_1n_1+b_2n_2+\cdots+b_kn_k(\bmod\ n_1)。\end{aligned}$$

记 s 是使 $a_s\neq b_s$ 的最大足标，即 $a_s\neq b_s$，$a_{s+1}=b_{s+1},\cdots$，$a_k=b_k$，那么有整数N使得

$$(a_1-b_1)n_1+(a_2-b_2)n_2+\cdots+(a_s-b_s)n_s=n_1N。\quad(*)$$

若记 $n_l=(n_1,\cdots,n_{s-1})m_l=(n_1,\cdots,n_s)d_sm_l(l=1,2,\cdots,s-1)$，又记 $n_s=(n_1,\cdots,n_s)c$。那么在(*)式两边除以公因数 $(n_1,\cdots,n_s)$ 后就得

$$(a_1-b_1-N)d_sm_1+\cdots+(a_{s-1}-b_{s-1})d_sm_{s-1}$$
$$+(a_s-b_s)c=0,$$
即有 $d_s|(a_s-b_s)c$。因为
$$\begin{aligned}(n_1,\cdots,n_{s-1},n_s)&=((n_1,\cdots,n_{s-1}),n_s)\\&=(d_s(n_1,\cdots,n_s),\ c(n_1,\cdots,n_s))\\&=(d_s,c)(n_1,\cdots,n_s),\end{aligned}$$
所以得 $(d_s,c)=1$，由此推出 $d_s|(a_s-b_s)$。但这与 $1\leqslant|a_s-b_s|<d_s$ 相矛盾。得证 $d_1d_2\cdots d_k$ 个和数 $a_1n_1+a_2n_2+\cdots+a_kn_k$ 对于模 n_1 互不同余。

【例 5】 一个整数 a 的 100 次方被 125 除，其余数可能是什么？即 $a^{100}\equiv b(\mathrm{mod}\ 125)$，试求 b 可能值有哪一些。

解 依同余分几种情况讨论。

若 $a=5k$，那么易见 $a^{100}\equiv 0(\mathrm{mod}\ 125)$；

若 $a=5k\pm1$，由于
$$a^{100}=(5k\pm1)^{100}=(5k)^{100}\pm100(5k)^{99}+\cdots\pm500k+1,$$
所以 $a^{100}\equiv1(\mathrm{mod}\ 125)$。

若 $a=5k\pm2$，由于
$$a^{100}=(5k\pm2)^{100}=(5k)^{100}\pm100(5k)^{99}+\cdots\pm500k\times2^{99}+2^{100},$$
所以 $a^{100}\equiv2^{100}(\mathrm{mod}\ 125)$。又由于
$$2^{100}=4^{50}=(5-1)^{50}=5^{50}-50\times5^{49}+\cdots-250+1,$$
所以 $2^{100}\equiv1(\mathrm{mod}\ 125)$，由此，按性质24即得 $a^{100}\equiv1(\mathrm{mod}\ 125)$。这样一来，便得 b 的可能值只能是 0（当 $5|a$）和 1（当 $5\nmid a$）。

最后，我们利用同余的性质来解 1978 年第二十届国际中学生数学竞赛第 1 题。

【例 6】 数 1978^n 与 1978^m 的最后三位数相等，试求出

正整数 n 和 m，使得 $n+m$ 取最小值，这里 $n>m\geq 1$。

解 按题意，

$$1978^n \equiv 1978^m \pmod{1000},$$

由性质 23 (ii)，

$$1978^n \equiv 1978^m \pmod 8,\quad 1978^n \equiv 1978^m \pmod{125}。$$

因 $1978=2\times 989$，而$(989,8)=1$，所以从第一式按性质 25 (ii) 得 $2^n \equiv 2^m \pmod 8$，由此即得 m 的最小值为 3。

又因 $(1978,5)=1$，所以从第二式再按性质 25(ii) 得

$$1978^{n-m} \equiv 1 \pmod{125}。$$

因为 $1978 \equiv 103 \pmod{125}$，由性质 23(ii)，$1978 \equiv 103 \equiv 3 \pmod 5$，易见 $3^4 \equiv 1 \pmod 5$，所以由性质 25(i)，$1978^4 \equiv 3^4 \equiv 1 \pmod 5$。这就是说必须 $n-m=4k$ 才有 $1978^{4k} \equiv 1 \pmod{125}$。

为确定 k 的最小值，注意到 $1978^4 = 25N+3^4 = 5q+1$，其中 $q=5N+16$，即 $5\nmid q$。这样

$$\begin{aligned} 1978^{4k}-1 &= (5q+1)^k-1 \\ &= 5^3\cdot b+\frac{k(k-1)}{2}5^2q^2+k\cdot 5q。\end{aligned}$$

因此要使 125 能整除左边，k 的最小值为 25。所以 $n-m=100$，$n+m=n-m+2m=106$。故 $n=103$，$m=3$ 是使 $n+m=106$ 取最小值的解。

习　题　12

1. (i) 试计算 $7^2 \equiv ?\pmod{10}$，$7^3 \equiv ?\pmod{10}$，$7^4 \equiv ?\pmod{10}$。

(ii) 若已知 $a \equiv -1 \pmod m$，问 $a^2 \equiv ?\pmod m$，$a^{2k} \equiv ?\pmod m$，$a^{2k+1} \equiv ?\pmod m$。

2. 试证 $63!\equiv 61!\ (\bmod 71)$。

3. (i) 若 $a\equiv b\ (\bmod m)$，d 是 a、b、m 的公因数，那么

$$\frac{a}{d}\equiv\frac{b}{d}\left(\bmod \frac{m}{d}\right)。$$

(ii) 若 $a\equiv b(\bmod m)$，试问 $a^2\equiv b^2(\bmod m^2)$ 是否成立？若成立试给出证明；若不成立试举出反例，又在 a、b 满足什么条件下才成立？

4. (i) 设整数 $N=\overline{a_na_{n-1}\cdots a_1a_0}$，试用同余性质证明 $11|N$ 当且仅当 $11\left|\sum\limits_{i=0}^{n}(-1)^ia_i[=(a_0+a_2+\cdots)-(a_1+a_3+\cdots)]\right.$。

(ii) 若记 $N=C_n1000^n+\cdots+C_11000+C_0$，那么 7，11，13 能整除 N 当且仅当

$$7\times 11\times 13\left|\sum_{i=0}^{n}(-1)^iC_i\right.。$$

5. 试证三个平方数的和对于模 8 不能与 7 同余，也即 $8k+7$ 型的正整数不能表示为三个整数的平方和。

6. 1979 年国庆 30 周年是星期一，问 2000 年的国庆是星期几？（注：1980 年是闰年，每四年一闰年）。

7. 试证若整数 n，$(n,10)=1$，那么 n^{101} 的末三位数码与 n 的末三位数码相同。（如 2123^{101} 的末三位数为 123，39^{101} 的末三位数码为 039。）

8. 若 a 是任意正奇数，证明 $a^{2^n}\equiv 1\ (\bmod 2^{n+2})$。

13. 剩余类及完全剩余组

在第 2 节中，我们把全体整数依其奇、偶性分成两类。自然会想到这种做法是否可以推广？现在利用同余概念，便可依下一原则把全体整数分为若干类：同类的数同余，非同类的数不同余。具体地说，对于某一给定的正整数 m，被 m 除时余数相同的整数划为一类。这样，如以 m 为模，我们便有 m 个类，这种类叫做关于模 m 的剩余类。例如 $m=2$ 时可分为两类：

R_0 类：$\cdots,-4,-2,0,2,4,\cdots,2n,\cdots$ 它们都对于模 2 与 0 同余，即 $2n\equiv 0 \pmod 2$。

R_1 类：$\cdots,-3,-1,1,3,\cdots,2n+1,\cdots$ 它们都对于模 2 与 1 同余，即 $2n+1\equiv 1 \pmod 2$。

易见，这个特例就是在 §2 讨论的偶数类 (R_0) 和奇数类 (R_1)。在一般 m 情形，所分成的 m 个类是：

$R_0=\{0\}$类：$\cdots,-2m,-m,0,m,2m,\cdots,km,\cdots$

$R_1=\{1\}$类：$\cdots,-2m+1,-m+1,1,m+1,2m+1,\cdots,km+1,\cdots$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$R_i=\{i\}$类：$\cdots,-2m+i,-m+i,i,m+i,2m+i,\cdots,km+i,\cdots$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$R_{m-1}=\{m-1\}$类：$\cdots,-m-1,-1,m-1,2m-1,3m-1,\cdots,(k+1)m-1,\cdots$

其中 R_i 就是由一切形如 $km+i$ $(k=0,\pm1,\pm2,\cdots)$ 的

整数所组成的一个集。显见，$R_0, R_1, \cdots, R_{m-1}$ 是关于模 m 的 m 个剩余类。

从上面可以看到，每一整数在且仅在一个剩余类中，在 R_i 中的整数对于模 m 都与 i 同余。这一点可以严格给出证明，这就是

性质 26 每一整数 a 在且仅在关于模 m 的一个剩余类中，又两个整数 a、b 在同一个剩余类中的充要条件是：

$$a \equiv b \pmod{m}。$$

证 给定整数 a，由带余除法的唯一性，对于模 m 可以唯一地写成 $a = mq + r$ 形式，此时 $a \equiv r \pmod{m}$，即 a 在且仅在类 R_r 中，

若 a、b 是属于 R_i 的两个不同的数，那么 $a = mq + i$，$b = mq' + i$，所以 $a \equiv i \equiv b \pmod{m}$。反之，当 $a \equiv b \pmod{m}$，那么由同余的定义，即知 a、b 必在同一个剩余类 R_i 中。

在 §2 中，对于 $m = 2$ 的特殊情形，我们给出过剩余类间的加法与乘法运算。运用同余性质可以证明，对于一般的 m 相应的结论也成立。限于篇幅我们不对一般的模 m 作详细论证了。

定义 剩余类 R_i 中的任一数 a 都可作为这一个类的"代表"，我们称它为该剩余类的一个剩余。若 $a_0, a_1, \cdots, a_{m-1}$ 是 m 个整数，且其中任两整数都不在同一剩余类中，则称 $a_0, a_1, \cdots, a_{m-1}$ 是模 m 的一个完全剩余组。

特别，以 $0, 1, \cdots, m-1$ 分别为 $R_0, R_1, \cdots, R_{m-1}$ 的"代表"，它们叫作模 m 的最小非负完全剩余组。

例如当 $m = 6$ 时，在 R_0 中取 0，R_1 中取 7，R_2 中取 -4，R_3 中取 15，R_4 中取 10，R_5 中取 5，那么 $0, 7, -4, 15, 10, 5$ 就组成模 6 的一个完全剩余组。通俗些说，每类派一个代表组

成的"全体代表团"就是一个完全剩余组。最小非负完全剩余组就是在每一类中取最小的非负整数为代表组成的全体代表团。

性质 27 (i) 要使 m 个整数构成模 m 的一个完全剩余组，当且仅当它们中两两(即任意两个)对于模 m 都不同余。

(ii) 任给 $m+1$ 个整数，其中至少有两数对于模 m 同余。

证 (i) 设给定 m 个整数 $b_1, b_2, \cdots, b_m$，若它们是模 m 的一个完全剩余组，由定义知其中任两数都不在同一个剩余类中，故由性质 26 即知 $b_i \not\equiv b_j \pmod m$，即两两对模 m 不同余。

反之，若 $b_1, b_2, \cdots, b_m$ 两两对模 m 不同余，所以由性质 26，它们分别含于相异的剩余类中，因此这 m 个数恰在 m 个不同的剩余类中。故 $b_1, b_2, \cdots, b_m$ 是一个完全剩余组。

(ii) 任给 $m+1$ 个整数，显然至少有两数落在 m 个剩余类 $R_0, R_1, \cdots, R_{m-1}$ 的某一类 R_i 中，由此按性质 26 此两数对于模 m 同余。

性质 27 粗看起来比较明显，但却是具有广泛应用的一个有力工具，现在我们应用它来解几个例子。

【例 1】 对任何正整数 n，都存在着仅由数码 1 和 0 组成的数 a，使得 $n \mid a$。

解 考察 $1, 11, \cdots, \overbrace{11\cdots1}^{n+1}$ 等 $n+1$ 个数。由性质 27 (ii)，这 $n+1$ 个数中至少有两数 $b=\overbrace{1\cdots1}^{l}$、$c=\overbrace{1\cdots1}^{k}$ $(l>k)$ 对于模 n 同余。由性质 23，$b\equiv c \pmod n$ 当且仅当 $n \mid (b-c)$，即 $n \mid \overbrace{1\cdots1}^{l-k}\ \overbrace{0\cdots0}^{k}$。

【例 2】 是否存在正整数 n，使得两数

$$a=\underbrace{11\cdots1}_{n}\underbrace{9\cdots9}_{n}\underbrace{7\cdots7}_{n}\underbrace{9\cdots9}_{n},$$

$$b=\underbrace{11\cdots1}_{n+1}\underbrace{9\cdots9}_{n+1}\underbrace{7\cdots7}_{n+1}\underbrace{9\cdots9}_{n+1}$$

都能被 1979 整除。

解 由上例知存在 n 使得 $1979|\overbrace{11\cdots1}^{n}\overbrace{0\cdots0}^{k}$，由于 $(10,1979)=1$，所以得 $1979|\overbrace{11\cdots1}^{n}$。从而

$$a=\overbrace{11\cdots1}^{n}(10^{3n}+9\times10^{2n}+7\times10^{n}+9)$$
$$\equiv 0\ (\mathrm{mod}\ 1979)$$

即 $1979|a$。又因

$$\overbrace{11\cdots1}^{n+1}\times10^{3n+3}=\overbrace{11\cdots1}^{n}\times10^{3n+4}+10^{3n+3}$$
$$=\overbrace{1\cdots1}^{n}\times10^{3n+4}+9\times\overbrace{1\cdots1}^{n}\times10^{3}+1000$$
$$\equiv 1000\ (\mathrm{mod}\ 1979)$$，同理可得

$$\overbrace{99\cdots9}^{n+1}\times10^{2n+2}\equiv900\ (\mathrm{mod}\ 1979),$$
$$\overbrace{77\cdots7}^{n+1}\times10^{n+1}\equiv70\ (\mathrm{mod}\ 1979),$$
$$\overbrace{99\cdots9}^{n+1}\equiv9\ (\mathrm{mod}\ 1979),$$

所以，$b\equiv1979\equiv0\ (\mathrm{mod}\ 1979)$，即 $1979|b$。

【例 3】 从数 1，2，$\cdots$200 中任选 101 个数，证明其中必有两个数，一个被另一个数整除。但可以选出 100 个数，使在其中没有一个数被另外 99 个数中任一个数整除。

证 将所选的 101 个数的标准分解式中 2 的乘幂去掉，余下就是奇数，这样共得 101 个奇数。但从 1 至 200 仅有 100 个奇数，所以在这 101 个奇数中必有两个奇数相同。这

就是说，原来所选的 101 个整数中有两数为 $2^k a$ 及 $2^l a$，a 为某奇数。若 $k<l$，那么 $2^k a | 2^l a$。

其次，我们来具体给出 1 至 200 中的 100 个数，其中任两数互相不能整除：

从 101，103，…，199 的 50 个奇数；

从 51，53，…，99 的奇数各乘以 2 有 25 个数；

从 27，29，…，49 的奇数各乘以 4 有 12 个数；

从 13，15，…，25 的奇数各乘以 8 有 7 个数；

从 7，9，11 三数各乘以 16 及 3×32，5×32，1×64 等共计 100 个数，易见这 100 个数无一数能被其中另一数整除。

在结束本节之前，我们利用剩余及完全剩余组来讨论数 a^k 被某数除的余数及 a^k 的末位数码等等，为此先证

性质 28 （费尔马定理） 设 p 是素数，a 是整数，且 $(a,p)=1$，那么

$$a^{p-1}\equiv1\pmod p。$$

证 先证 $a,2a,\cdots,(p-1)a$ 是 $p-1$ 个对于模 p 互不同余的整数，因若不然有 $la\equiv ka\pmod p$ $(1\leqslant l<k\leqslant p-1)$，那么 $(k-l)a\equiv0\pmod p$，即 $p|(k-l)a$。由于 $(p,a)=1$，故 $p|(k-l)$，这不可能，所以 $la\not\equiv ka\pmod p$。

因为 $(a,p)=1$，所以 $a,2a,\cdots,(p-1)a$分别属于关于模 p 的剩余类 R_1，R_2，…，R_{p-1}，即在适当改变 1，2，…，$p-1$ 的顺序为 i_1，i_2，…，i_{p-1}，后有

$a\equiv i_1\pmod p$，$2a\equiv i_2\pmod p$，…，$(p-1)a\equiv i_{p-1}\pmod p$，从而，按性质 25(i)，有

$$a\times2a\times\cdots\times(p-1)a\equiv i_1i_2\cdots i_{p-1}\pmod p,$$

即

$$(p-1)!\,a^{p-1}\equiv(p-1)!\pmod p。$$

由于 $(p,(p-1)!)=1$，故得 $a^{p-1}\equiv1\pmod p$。

用费尔马定理可以更简单地证明第 9 节例 8，读者可以一试。

【例 4】 设 p 是素数，a 是正整数，$(a,p)=1$，试证：

(i) 存在正整数 k，$1\leqslant k\leqslant p-1$，使得 $a^k\equiv 1\pmod p$；

(ii) 记满足 $a^k\equiv 1\pmod p$ 的最小正整数为 k_0，则 $k_0|(p-1)$。

证 由所给条件，按性质 28 即知 (i) 成立。

设 k_0 是满足 (ii) 中条件的最小正整数，记 $p-1=k_0q+r$，$0\leqslant r<k_0$。由假设及性质 28，有

$$a^{k_0}\equiv 1\pmod p \text{ 及 } a^{p-1}\equiv 1\pmod p。$$

又因 $a^{p-1}=a^{k_0q+r}=(a^{k_0})^qa^r$，所以

$$a^r\equiv a^r\cdot(a^{k_0})^q\equiv a^{p-1}\equiv 1\pmod p,$$

即 $a^r\equiv 1\pmod p$。因 k_0 是满足 $a^k\equiv 1\pmod p$ 的最小正整数，所以必须 $r=0$，由此 $p-1=k_0q$，可知 $k_0|(p-1)$。

注 本例中的 k_0 未必为 $p-1$，如 $p=7$：

$$4^3\equiv 1\pmod 7 \text{ 此时 } k_0=3,$$

$$6^2\equiv 1\pmod 7 \text{ 此时 } k_0=2。$$

【例 5】 试计算

$$10^{10}+10^{10^2}+\cdots+10^{10^{10}}$$

被 7 除的余数。

解 由性质 28，$10^6\equiv 1\pmod 7$，再由性质25，$10^{6k}\equiv 1^k\equiv 1\pmod 7$。而

$$10\equiv 4\pmod 6, 10^2\equiv 4\pmod 6,\cdots,10^{10}\equiv 4\pmod 6,$$

即 $10^l=6k+4$。所以 $10^{10^l}\equiv 10^4\pmod 7$，由此，

$$10^{10}+10^{10^2}+\cdots+10^{10^{10}}\equiv 10^4+10^4+\cdots+10^4$$
$$=10^5\pmod 7。$$

而 $10^5=7\times 14285+5$，即 $10^5\equiv 5\pmod 7$，所以所求的余数为 5。

【例 6】 求 $25^{35^{45}}$ 被 13 除的余数。

解 由于 $25\equiv 12 \pmod{13}$ 及 $25^2\equiv 1 \pmod{13}$，所以

$$25^{2k}\equiv 1 \pmod{13},\quad 25^{2k+1}\equiv 25\equiv 12 \pmod{13}。$$

易见 $35^{45}=2N+1$ 为奇数，所以得 $25^{35^{45}}$ 被 13 除的余数为 12。

【例 7】 试找出 7^{7^7} 及 $17^{17^{17}}$ 的个位数码。

解 由于 $7^2\equiv -1 \pmod{10}$，$7^3\equiv 3 \pmod{10}$，所以 $7^4\equiv 1 \pmod{10}$。又因

$$7\equiv 3 \pmod 4,\quad 7^6\equiv 1 \pmod 4,\quad 7^7\equiv 3 \pmod 4$$

所以 $7^7=4k+3$，由此即得

$$7^{7^7}\equiv 7^{4k+3}\equiv (7^4)^k 7^3\equiv 3 \pmod{10},$$

故知，7^{7^7} 的末位数码为 3。

由于 $17^2\equiv -1 \pmod{10}$，$17^4\equiv 1 \pmod{10}$。又因

$$17\equiv 1 \pmod 4,\quad 17^{17}\equiv 1^{17}\equiv 1 \pmod 4,$$

所以 $17^{17}=4k+1$。由此即得

$$17^{17^{17}}\equiv 17^{4k+1}\equiv (17^4)^k\times 17\equiv 1\times 17\equiv 7 \pmod{10},$$

故知，$17^{17^{17}}$ 的末位数码为 7。

【例 8】 试求 $\overbrace{7^{7^{\cdots^{7}}}}^{k}$ 的末两位数码 $(k\geqslant 2)$。

解 首先

$$7^2\equiv 49 \pmod{100},\quad 7^3\equiv 43 \pmod{100},\quad 7^4\equiv 1 \pmod{100}。$$

所以 $7^{4m}\equiv 1 \pmod{100}$。另一方面：

$$7\equiv 3 \pmod 4,\quad 7^2\equiv 1 \pmod 4,$$

所以 $7^{2l+1}\equiv 3 \pmod 4$。显然 $\overbrace{7^{7^{\cdots^{7}}}}^{k-1}=7^{2l+1}$，其中 l 为正整数。于是

$$\overbrace{7^{7^{\cdots^{7}}}}^{k-1}\equiv 3 \pmod 4 \quad 即 \quad \overbrace{7^{7^{\cdots^{7}}}}^{k-1}=4m+3。$$

因此我们有

$$\overbrace{7^{7^{\cdots^{7}}}}^{k} = 7^{4m+3} \equiv 7^3 \equiv 43 \pmod{100},$$

即得所求数的末两位数码为 43。

关于剩余组、同余方程的求解等等不在此一一详述，有兴趣的读者请参阅有关著作。

习　题　13

1. 试证存在正整数 n，使得 $131 \mid \overbrace{11\cdots1}^{n}$。

2. 试证：对于素数 p，$(p,10)=1$，存在正整数 n 使得 $p \mid \overbrace{11\cdots1}^{n}$。

3. 设正整数 a、m，$(a,m)=1$，那么

$$a, 2a, 3a, \cdots, ma$$

是模 m 的一个完全剩余组。

4. 设 $a_1, a_2, \cdots, a_m$ 是模 m 的完全剩余组，若 $(k,m)=1$，那么

$$ka_1+l,\ ka_2+l,\ \cdots,\ ka_m+l$$

是模 m 的一个完全剩余组。

5. 从数 1，2，$\cdots$，100 中任选 51 个数，证明其中必有两个数，一个被另一个数整除。但可选出 50 个数，使其中没有一个数被其余 49 个中任一个数整除。

6. 试求 $7^{17^{27}}$ 的末位数码。

7. 试求 $21^{21^{21}}$ 被 11 除的余数。

8. 试求 3^{999} 的末两位数码。

习 题 解 答

习题 1

1.2.3.4. 由整除性的定义仿性质 1、2 的证明即得。

5. 由于已知 $(m-p)|(mn+pq)$ 及

$$(mn+pq)-(mq+np)=(m-p)(n-q),$$

故由 4. 即得 $(m-p)|(mq+np)$。

6. 若 a、b 中有一数是 3 的倍数，那么 ab 是 3 的倍数。若 a、b 都不是 3 的倍数，由例 2 已知 $a+b$、$a-b$ 中有且仅有一个是 3 的倍数。故得证 $a+b$、$a-b$ 及 ab 中至少有一个是 3 的倍数。(注意，仅当 a、b 都是 3 的倍数时，三者都是 3 的倍数；其余情形，三者有且仅有一个是 3 的倍数。)

习题 2

1. (从略)

2. 注意每发生一次握手，对于握手的两人是各握手一次，但握手的人次来说恰为 2 次，故握手总数(人次)必为偶数。

3. (从略)

4. 写 $a=2n+1$，故 $a^2-1=4n(n+1)$。已知 $2|n(n+1)$，由习题 1 第 2 题得 $2\times4|4n(n+1)$，即 $8|(a^2-1)$。

5. 显见 a 与 a^3 的奇偶性相同，故 $a-1$ 与 a^3-1 的奇偶性相同。同样，b 与 b^3 的奇偶性相同，故 $a\pm b$ 与 $a^3\pm b^3$ 的奇偶性相同。

6. 一般情形是：任给 $2n+1$ 个整数 $a_1, a_2, \cdots, a_{2n+1}$，把它们按任意顺序编排，得 $b_1, b_2, \cdots, b_{2n+1}$，那么

$$(a_1-b_1)(a_2-b_2)\cdots(a_{2n+1}-b_{2n+1})$$

是偶数。证明方法与例 3 类同，把 $2n+1$ 个整数 $a_1, a_2, \cdots, a_{2n+1}$ 按奇、偶分类，至少有 $n+1$ 个属同一类。不妨设 $a_1, a_2, \cdots, a_{n+1}$ 属同一类，那么在 $b_1, b_2, \cdots, b_{n+1}$ 中也至少有一个与它们同属一类，由此即得 $(a_1-b_1)(a_2-b_2)\cdots(a_{2n+1}-b_{2n+1})$ 是偶数。

7. 一般情形是：能否把奇数只电话用电线把其中每只恰与另奇数只电话连接成直通电话。回答是否定的，证明从略。

8. 不能作出这样的安排。若不然，可作这样安排的话，设总的比赛场次为 k 场，因每一场比赛由二个队进行，所以出场比赛的共有 $2k$ 个队次。另一方面每个队都恰好参加奇数次比赛，29 个奇数之和还是奇数，即总计参加比赛的队次为奇数次，与 $2k$ 为偶数相矛盾。

9. 不能作出这样安排，证明从略。

10. 若有这样的凸多面体，设它有 n 条棱，每一条棱与凸多面体的两个面相连，这样与 n 条棱相邻的面共有 $2n$ 个。另一方面，每个面是奇数边形，故每一个面总与奇数个面相邻，奇数个面总共相邻也为奇数次，与 $2n$ 为偶数相矛盾。故得证不存在这样的凸多面体。

11. 若不然，设有整数根 x_0，故

$$f(x_0)=a_0x_0^n+a_1x_0^{n-1}+\cdots+a_{n-1}x_0+a_n=0,$$

所以 $x_0|a_n$。因假设 $a_n=f(0)$ 是奇数，所以 x_0 也是奇数。又已知 $f(1)=a_0+a_1+\cdots+a_n$ 是奇数，而 a_i 与奇数 x_0^{n-i} 的积 $a_ix_0^{n-i}$ 是与 a_i 有相同的奇偶性的，所以 $f(x_0)$ 与 $f(1)=a_0+a_1+\cdots+a_n$ 有相同的奇偶性，即 $f(x_0)$ 为奇

数，这与 $f(x_0)=0$ 矛盾。得证 $f(x)$ 无整数根。

习题 3

1. 解法与例 1 相同。由二项展开式有

$$\begin{aligned}(x+y)^7 &= x^7+7x^6y+21x^5y^2+35x^4y^3+35x^3y^4 \\ &\quad +21x^2y^5+7xy^6+y^7 \\ &= x^7+y^7+7xy(x^5+y^5) \\ &\quad +21x^2y^2(x^3+y^3)+35x^3y^3(x+y)\end{aligned}$$

由假设知 $7|(x+y)$，而 x^5+y^5，x^3+y^3 都有因式 $x+y$，所以上式右边最后三项都能被 7^2 整除。因此按习题 1 第 4 题可知 49 能整除 x^7+y^7。

2. 利用因式分解，我们有

$$\begin{aligned}N &= (2^2-1)(2^8+2^4+1)=(2^2-1)(2^4+2^2+1) \\ &\quad \times(2^4-2^2+1)。\end{aligned}$$

易见 $2^2-1=3$，$2^4+2^2+1=21$，故得证 $9|N$。

3. 由 $6^{2n}-1=36^n-1=35(36^{n-1}+36^{n-2}+\cdots+1)$ 即得。

4. 因 $1978=1979-1, 1980=1979+1$，故

$$1978^{1978}=(1979-1)^{1978}=1979M_1+1,$$

$$1980^{1979}=(1979+1)^{1979}=1979M_2+1,$$

$$\begin{aligned}1978^{1978}+1980^{1979}-1981 &= 1979(M_1+M_2)+2 \\ &\quad -1981=1979(M_1+M_2-1)。\end{aligned}$$

5. 记 $n=2k$，那么

$$\begin{aligned}13^n+6 &= 13^{2k}-1+7=169^k-1+7=168M+7 \\ &= 7(24M+1)。\end{aligned}$$

6. 因为 $p=(p-1)+1$，所以

$$\begin{aligned}\text{原式} &= [(p-1)+1]^n+(p-1)(p-2)n-1 \\ &= [(p-1)^n+n(p-1)^{n-1}+\cdots \\ &\quad +C_n^2(p-1)^2+n(p-1)+1]\end{aligned}$$

$$+(p-1)(p-2)n-1$$
$$=(p-1)^2[(p-1)^{n-2}+\cdots+C_n^2]$$
$$+\{n(p-1)+1+(p-1)(p-2)n-1]$$
$$=(p-1)^2[(p-1)^{n-2}+\cdots+C_n^2]$$
$$+n(p-1)^2$$
$$=(p-1)^2[(p-1)^{n-2}+\cdots+C_n^2+n]。$$

7. 注意到

$$a^{n+1}-(a-1)n-a$$
$$=(a-1)(a^n+a^{n-1}+\cdots+a-n)$$
$$=(a-1)^2[(a^n-1)+(a^{n-1}-1)+\cdots+(a-1)]$$
$$=(a-1)^2(a^{n-1}+2a^{n-2}+\cdots+n)。$$

本题也可用第6题的方法解，而第6题也可用本题的方法解。

显然，第5、6、7三题都可对指数 n 用数学归纳法证明之。

8 （从略）

9. (i) 对指数用数学归纳法即可。

(ii) 用数学归纳法。当 $n=1$ 时

$$a^{l+1}+b^{l+1}+c=a(a^l-b^l)+b^l(a+b+c)$$
$$-c(b^l-1),$$

由已知条件即得 $d|(a^{l+1}+b^{l+1}+c)$。假设当 $n=k$ 时命题成立，当 $n=k+1$ 时，

$$a^{l(k+1)+1}+b^{l(k+1)+1}+c$$
$$=a^l(a^{lk+1}+b^{lk+1}+c)-b^{lk+1}(a^l-b^l)$$
$$-c[(a^l-b^l)+(b^l-1)]$$

由已知条件及假设得证 $d|[a^{l(k+1)+1}+b^{l(k+1)+1}+c]$。

习题4

1. $(10231,1820)=13$。

2. 由性质 7 知存在整数 k、l，使得 $(a,b)=ka+lb$，若 c 是 a、b 的公因数，则 $c|a$，$c|b$，所以 $c|(ka+lb)$，即得 $c|(a,b)$。

3. 记 $d_1=(a_1, a_2, a_3)$，$d_2=((a_1, a_2), a_3)$。因 d_1 是 a_1,a_2,a_3 的最大公因数，由上一题知 $d_1|(a_1,a_2)$，再由上一题知 $d_1|((a_1,a_2),a_3)$，即 $d_1|d_2$。另一方面，$d_2|(a_1,a_2)$，$d_2|a_3$，又由 $d_2|(a_1,a_2)$ 知 $d_2|a_1$，$d_2|a_2$，即 d_2 也是 a_1,a_2,a_3 的公因数，所以 $d_2|(a_1,a_2,a_3)=d_1$。由是即得 $d_1=d_2$。

4. 因 $a=cq+r$，$b=cq_1+r_1$，多次运用第 3 题及性质 5 可得

$$\begin{aligned}(a,b,c)&=((a,c),b)=((c,r),b)=(c,b,r)\\&=((b,c),r)=((c,r_1),r)=(c,r,r_1).\end{aligned}$$

5. 记 $(a,b)=d$，$(am,bm)=d'$。按性质 7，存在整数 k，l 使得 $(a,b)=ka+lb$。所以

$$kam+lbm=dm.$$

因此 $d'|dm$，即 $d'\leqslant dm$。另一方面，$d|a$，$d|b$，所以 $dm|am$，$dm|bm$。由此按第 2 题 $dm|(am,bm)$，即 $dm|d'$，$dm\leqslant d'$，故得证 $d'=dm$。

6. 因 $a>1$，$b>1$，$(a,b)=1$，由性质 7 知存在整数 k,l' 使得 $ka+l'b=1$。不妨设 $k>0$，因此 $l'<0$，记 $l=-l'>0$，即有 $ka-lb=1$。令 $k=bq+\xi$，$0<\xi<b$（这里 $\xi\neq 0$，否则 $baq-lb=1$，$b|1$，但已设 $b>1$，矛盾）。代入得

$$1=a\xi+abq-lb=a\xi-b(l-aq).$$

记 $\eta=l-aq$，即有 $a\xi-b\eta=1$。现在只需证 $0<\eta<a$。因 $a>1$，$\xi\geqslant 1$，故 $b\eta=a\xi-1>0$，又 $b>1$，所以证得 $\eta>0$。另外，$\xi<b$，故 $a\xi<ab$，由此得

$$b\eta=a\xi-1<a\xi<ab,$$

由 $b>1$，又证得 $\eta<a$。

7. 前者显然。由性质 7 知若 $(a,b)=d$，那么有整数 k、l 使 $ka+lb=d$。但后者就未必成立，如 $6\times10-4\times14=4$，但 $(6,4)=2\neq4$。

8. 记 $d=ax_0+by_0$，对任一形如 $ax+by$ 的数，当它用 d 除时，有 $ax+by=dq+r$，$0\leqslant r<d$。而

$$r=ax+by-dq=ax+by-(ax_0+by_0)q$$
$$=a(x-x_0q)+b(y-y_0q),$$

即 r 也是具有 $ax'+by'$ 形状的非负整数，由假设 d 是 $ax+by$ 形中最小正数，因此 $r=0$。即得对任何 x、y，$d|ax+by$。

不妨设 $a>0$，$b>0$。当 $x=1$，$y=0$ 即得 $d|a$，又当 $x=0$，$y=1$ 即得 $d|b$。所以 $d=(ax_0+by_0)|(a,b)$。显然 $(a,b)|ax_0+by_0$，故得证 $(a,b)=ax_0+by_0$。

9. 记 $d=(a+b,\ a^2+b^2)$。因为

$$2a^2=a^2+b^2+(a+b)(a-b),$$
$$2b^2=a^2+b^2-(a+b)(a-b)。$$

所以 $d|2a^2$，$d|2b^2$，因此得 $d|(2a^2,2b^2)$。但由第 5 题及假设知 $(2a^2,2b^2)=2(a^2,b^2)=2$，即 $d|2$，所以得证 $d=1$ 或 2。

10. 写 $\sqrt[n]{a}=p/q$，$(p,q)=1$，即有 $aq^n=p^n$，由此 $q|p^n$。但 $(p,q)=1$，所以得 $q=1$。因此若 $\sqrt[n]{a}$ 为有理数，那么必为整数，否则就为无理数。

习题 5

1 (i). 写 $n=2k$，由

$$n^3-28n=8(k-1)k(k+1)-48k$$

按例 1 即知 $48|(n^3-28n)$。

(ii). 写

$$n^2(n^2-1)=(n-1)n\cdot n(n+1)。$$

因 $2|(n-1)n$，$2|n(n+1)$，$3|(n-1)n(n+1)$，即得 $12|n^2(n^2-1)$。

(iii). 因为

$$n(n^2-1)(3n+2)$$
$$=2n^2(n^2-1)+(n-1)n(n+1)(n+2),$$

由(ii)及 $24|(n-1)n(n+1)(n+2)$
即得 $24|n(n^2-1)\times(3n+2)$。

(iv) 因为

$$n(n^2-49)(n^2+49)$$
$$=n(n^2-1)(n^2-4)+5n(n^2-1)-2400n,$$

而右边每一项都能被 30 整除，故得 $30|n(n^2-49)(n^2+49)$。

2. 由于

$$a_1^3+a_2^3+a_3^3-(a_1+a_2+a_3)=a_1(a_1^2-1)$$
$$+a_2(a_2^2-1)+a_3(a_3^2-1)。$$

已知 $6|n(n^2-1)$，所以上式右边是 6 的倍数，又已知 $6|(a_1+a_2+a_3)$，所以 $6|(a_1^3+a_2^3+a_3^3)$。

3. 由例 2 已知此时 $24|(a_1^2-1)$，$24|(a_2^2-1)$，所以有 $24|[(a_1^2-1)-(a_2^2-1)]$，即 $24|(a_1^2-a_2^2)$。

4. 记 $S=1^5+2^5+\cdots+9^5$，那么

$$2S=2(1^5+2^5+\cdots+9^5)$$
$$=(1^5+9^5)+(2^5+8^5)+\cdots+(9^5+1^5)$$
$$=10N,$$

其中N为某自然数。另一方面

$$2S=(0^5+9^5)+(1^5+8^5)+\cdots+(9^5+0^5)=9M,$$

其中M为某自然数，由于 $(9,10)=1$，所以 $90|2S$，即得 $45|S$，而 $(1+2+\cdots+9)=45$。一般地，对于正奇数 k 有

$$(1+2+\cdots+n)|(1^k+2^k+\cdots+n^k)。$$

5. 把 a、b、c、d 按奇偶分类，或两两在同一类，或至少有

三个在一类，此时都有

$$4|(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)。$$

又用 3 除时，a、b、c、d 四数至少有两数的余数相同，所以该乘积又能被 3 整除，由此即得 12 能整除这一乘积。

6．当 $k=2l+1$ 时，

$$n^k-n=n(n^{2l}-1)=n(n^2-1)(n^{2(l-1)}+\cdots+1)。$$

所以由 $6|n(n^2-1)$，即得 $6|(n^k-n)$。又若 n 也为奇数，记 $n=2m+1$，此时

$$\begin{aligned}n(n^2-1)&=2m(2m+1)(2m+2)\\&=4m(m+1)(m+2)+4(m-1)\times\\&\quad m(m+1),\end{aligned}$$

即得 $24|n(n^2-1)$，所以有 $24|(n^k-n)$。

7．因为 $n^2+8n+15=(n+4)^2-1$。若 $(n+4)|(n^2+8n+15)$，那么就有 $(n+4)|1$，这是不可能的。

8．因为

$$2^{3m}=7k+1,\ 2^{3m+1}=7k+2,\ 2^{3m+2}=7k+4。$$

所以不论 n 被 3 除余数是多少，2^n+1 被 7 除的余数不能的 0，即 $7\nmid(2^n+1)$。

9(i)．若有 $1\leqslant i<j\leqslant K$，使 $K|(iM-jM)$，即 $K|(i-j)M$，由 $(K,M)=1$，即得 $K|(i-j)$，这是不可能的。

(ii)．由(i)知，数 M、$2M$、$\cdots$、KM 除以 K 时所得余数两两不同。若 $N=Kq+r$，那么有 $1\leqslant l\leqslant K$ 使 $lM=Kq'+(K-r)$，那么 $N+lM=K(q+q'+1)$，即得证 $K|(N+lM)$。

10．(i)、(ii) 显然成立。对于 (iii) 记 $(a,b)=d$，$[a,b]=ab/(a,b)$。所以

$$b[a,a+b]=\frac{b\cdot a(a+b)}{(a,a+b)}$$
$$=\frac{(a+b)\cdot ab}{(a,b)}$$
$$=(a+b)[a,b]。$$

习题 6

1. 由 $n(2n+1)(n-5)$
$$=(2n+1)n(n+1)-6n(2n+1)$$
$$=(n-1)n(n+1)+n(n+1)(n+2)$$
$$-6n(2n+1)。$$

即得 $6\mid n(2n+1)(n-5)$。

2.
$$n^2(2n^4+3n^3-n^2-3n-1)$$
$$=n^2(n+1)^2(n-1)(2n+1)$$
$$=n^2(n+1)^2(n-1)^2$$
$$+(n-1)n^2(n+1)^2(n+2),$$

已知 $(3!)^2\mid n^2(n+1)^2(n-1)^2$，$6\mid(n-1)n(n+1)$，$6\mid n\times(n+1)(n+2)$，由此即得 36 能整除左边。

3. 注意到 $8640=2^6 3^3 5$，
$$n^3(n^6-6n^4+9n^2-4)=n^3(n^2-1)^2(n^2-4)$$
易见 $5\mid n(n^2-1)(n^2-4)$，$3\mid(n-1)n(n+1)$，$3\mid n(n-1)(n-2)$，$3\mid n(n+1)(n+2)$。又不论 n 为偶数(此时可分 $n=4k$ 与 $n=4k+2$ 讨论，都有 $2^4\mid n^3(n^2-4)$) 或 n 为奇数 $8^2\mid(n^2-1)^2$，所以都有 $2^6\cdot3^3\cdot5\mid n^3(n^6-6n^4+9n^2+4)$。

4. 因为
$$2l(2l+2)\cdots(2l+2k-2)$$
$$=2^k\cdot l(l+1)\cdots(l+k-1),$$
已知 $k!\mid l(l+1)\cdots(l+k-1)$，故得 $2^k(k!)$ 能整除相继

k个偶数的乘积。

5. 因为

$$f(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$
$$= \frac{1}{6}n(n+1)(2n+1)。$$

6. 因为

$$f(n) = \frac{2}{5}n^5 - \frac{1}{3}n^3 - \frac{1}{15}n$$
$$= \frac{1}{15}n(n^2-1)(6n^2+1)$$
$$= \frac{1}{3}n(n^2-1)(n^2+1)$$
$$+ \frac{1}{15}n(n^2-1)(n^2-4)。$$

7. 注意到

$$\frac{(m+n-1)!}{(m-1)!n!} = C_{m+n-1}^{n},$$
$$\frac{(m+n-1)!}{m!(n-1)!} = C_{m+n-1}^{m}$$

都是整数，即有整数 Q, Q' 使得

$$(m+n-1)! = m!(n-1)!Q = (m-1)!n!Q'。$$

所以

$$m\cdot(m+n-1)! = m!n!Q'$$
$$= m\cdot m!(n-1)!Q,$$

由此得 $nQ' = mQ$。因 $(n,m)=1$，所以 $n|Q$，即有 $Q = nQ''$，代入得 $(m+n-1)! = m!n!Q''$，得证

$$m!n!|(m+n-1)!。$$

8. 在 $a+b+\cdots+k \leqslant n$ 时，写

$$\frac{n!}{a!b!\cdots j!k!}=\frac{n(n-1)\cdots(n-a+1)}{a!}$$
$$\times\frac{(n-a)\cdots(n-a-b+1)}{b!}\cdots$$
$$\times\frac{(n-a-b-\cdots-j)\cdots2\times1}{k!}$$

由 $n-a-\cdots-j\geqslant k$，所以上式右边每一项都是整数，故得证左边也是整数。

9．首先因 $m>1$，故对于 $l\geqslant 0$，$m^l\geqslant 2^l\geqslant l+1$。由此得 $m^n\geqslant n+1\geqslant k$。写成

$$C_{m^n}^k=\frac{m^n\times(m^n-1)\times\cdots\times(m^n-i)\times\cdots\times(m^n-k+1)}{k\times1\times\cdots\times i\times\cdots\times(k-1)}。$$

若 $i=m^rq$，$m\nmid q$，那么 $m^n-i=m^r(m^{n-r}-q)$，所以 i 和 m^n-i 含 m 的相同方幂 m^r。同样，若 p 是 m 的素因数，i 和 m^n-i 含 p 的方幂也相同。又由于 $m^{k-1}\geqslant k(k\geqslant 1)$，即 k 中 m 的幂次至多为 m^{k-1}，所以 $m^{n-(k-1)}=m^{n-k+1}$ 必能整除 $C_{m^n}^k$。

习题 7

1．注意当 p 为素数时 $p\mid C_p^k(k=1,\cdots,p-1)$。所以由

$$(a+b)^p-a^p-b^p=C_p^1ab^{p-1}+C_p^2a^2b^{p-2}+\cdots$$
$$+C_p^1a^{p-1}b$$

即得 $p\mid[(a+b)^p-a^p-b^p]$。

2．当 $n>1$ 时，由于

$$n^4+4=(n^2-2n+2)(n^2+2n+2)$$

是两个大于 1 的整数的乘积，所以此时 n^4+4 为合数。

3．因 p 为大于 5 的素数，所以 $p\neq 3k$；又 $p\neq 3k+1$

(否则 $2p+1=6k+3$ 就不是素数)。由此即得 $p=3k+2$。此时 $4p+1=12k+3=3(4k+1)$ 是合数。

4. 当 p 是大于 3 的素数时，必有 $p=6k\pm1$ 的形式。所以

$$p^2=12(3k^2\pm k)+1。$$

5. 写 $m=3i+1$，$n=3j+2$。当 $a\neq 3k$ 时，若 $a=3k+1$，那么 $a+n=3(k+j+1)$ 不是素数；若 $a=3k+2$，那么 $a+m=3(k+i+1)$ 也不是素数。

6. $p=3$ 时，$8p^2+1=73$ 也是素数，所以 $p=3$ 是一解。此外无解，因为 $p=3k\pm1$ 时，

$$8p^2+1=72k^2\pm48k+9=3(24k^2\pm16k+3)$$

是合数。

7. $p=3$ 是一解，此外无别的解，因若 $p=3k+1$ 时，$p+14=3k+15=3(k+5)$ 为合数；若 $p=3k+2$ 时，$p+10=3k+12=3(k+4)$ 是合数。

8. 只要写出 $n^2+3n+5=(n+7)^2-11(n+4)$，仿照例 5 同样可证。

9. 记不大于 n 的素数为 $p_1,\cdots,p_k$，记 $q=p_1\cdots p_k-1$。因 $n>2$，所以 $q>4$。易证 q 有一个不同于 $p_1,\cdots,p_k$ 的素因数 p，所以 $p>n$。又 $p\leqslant q\leqslant n!-1<n!$。这就证明了在 n 与 $n!$ 之间有素数 p。

10. 取这样的素数 p，使得 $\frac{2}{p}<\min\limits_{0\leqslant i\leqslant n-1}(x_{i+1}-x_i)$。由此，在每一区间 $[x_i, x_{i+1}]$ 中至少有两个形如 k/p 的数。不妨记这种相邻两分数为 k/p，$(k+1)/p$。由于

$$\frac{k}{p}=\frac{kp}{p^2}<\frac{kp+1}{p^2}<\frac{kp+p}{p^2}=\frac{k+1}{p}$$
$$(0\leqslant k\leqslant p-1)。$$

$(kp+1,\ p^2)=1$，所以 $(kp+1)/p^2$ 是在给定分数 k/p，$(k+1)/p$ 之间(当然更在 $[x_i, x_{i+1}]$ 之间)的不可约分数，且 $m=p^2$ 是合数，得证命题成立。

习题 8

1. $1000027=100^3+3^3=103\times73\times19\times7$。

2. $\sqrt[m]{n}=p_1^{\frac{\alpha_1}{m}}p_2^{\frac{\alpha_2}{m}}\cdots p_k^{\frac{\alpha_k}{m}}$。当 $m|\alpha_i(i=1,\cdots,k)$ 时，显然 $\sqrt[m]{n}$ 为正整数。反之当 $\sqrt[m]{n}=a$ 为正整数时，那么可有

$$a^m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}。$$

又由于 a 是正整数，故也有标准分解

$$a=p_1^{\beta_1}\cdots p_k^{\beta_k},$$

由标准分解的唯一性知 $\alpha_i=m\beta_i(i=1,\cdots,k)$，即得证 $m|\alpha_i$。

3. 事实上若 $\log_m n=s/r$，即 $m^{s/r}=n$，$m^s=n^r$。所以有

$$p_1^{\beta_1 s}p_2^{\beta_2 s}\cdots\cdots p_k^{\beta_k s}=p_1^{\alpha_1 r}p_2^{\alpha_2 r}\cdots\cdots p_k^{\alpha_k r}。$$

上式成立的充要条件是

$$\beta_i s=\alpha_i r\ (i=1,2,\cdots k),$$

即
$$\beta_1/\alpha_1=\beta_2/\alpha_2=\cdots=\beta_k/\alpha_k=r/s。$$

4. 仿照例 4 同样可证。

5. 当 $m=ab$；$1<a\leqslant b<m$ 且 $m\geqslant6$ 时，若 $a\neq b$，那么 $(m-1)!$ 中有数 a 及 b，所以 $m=ab|(m-1)!$；若 $a=b$，那么 $m=a^2\geqslant6$，所以 $a>2$，$2a<a^2$，因此 $2a\leqslant a^2-1=m-1$。即在 $(m-1)!$ 中有数 a 及 $2a$，所以 $m=a^2|(m-1)!$

反之，当 $m=p$ 为素数时 $p\nmid(p-1)!$。当 m 为 $\leqslant5$ 的合数即 4 时显然 $m\nmid(m-1)!$。

6. 设 k 是满足 $2^k \leqslant n$ 的最大整数，P 为所有 $\leqslant n$ 的奇数的乘积。那么在 $2^{k-1}PS_n$ 中除去 $\frac{1}{2^k}2^{k-1}P$ 这一项为分数外，其余各项都为整数。所以 $2^{k-1}PS_n$ 不为整数，即 S_n 不可能是整数。

7. $C_{2^n}^{2^k-1}=\frac{2^n!}{(2^k-1)!(2^n-2^k+1)!}$。

由于

$$
\begin{aligned}
2^n! &= 2^n(2^n-2)\cdots 2\times P_n \\
&= 2^{2^{n-1}}P_n\times 2^{n-1}! = \cdots \\
&= 2^{2^n-1}P_nP_{n-1}\cdots P_1。
\end{aligned} \quad (1)
$$

$$(P_n = 1\times 3\times\cdots\times(2^n-1))$$

所以

$$(2^k-1)! = 2^k!/2^k = 2^{2^k-k-1}P_1\cdots P_k。$$

再看

$$(2^n-2^k+1)! = (2^n-2^k+1)\times(2^n-2^k)!,$$

用与(1)同样的论证方法可知，在 $(2^n-2^k)!$ 中含 2 的方幂数为

$$
\begin{aligned}
&2^{k-1}(2^{n-k}-1)+\cdots+(2^{n-k}-1)+(2^{n-k-1}-1) \\
&\quad +\cdots+(2-1) = 2^n-2^k-n+k
\end{aligned}
$$

所以在 $C_{2^n}^{2^k-1}$ 中 2 的方幂数为

$$2^n-1-(2^k-k-1)-(2^n-2^k-n+k)=n$$

这就是说 $2^n | C_{2^n}^{2^k-1}$，而 2^{n+1} 不能整除它。

习题 9

1. 我们来证数列 $1,2,\cdots,(10^n-1)$ 的一切数中各个数码之和为 $45n\times 10^{n-1}$。

事实上，当 $n=1$ 时，$1,2,\cdots,9$ 的数码和为 45，命题成

立。归纳假设当 $n=k-1$ 时，命题正确。当 $n=k$ 时，考察

$$1,2,\cdots,10^{k-1}-1;\ 10^{k-1},\cdots,2\times10^{k-1}-1;\cdots;$$
$$9\times10^{k-1},\cdots,10^{k}-1。$$

在这十组中，若不计后九组中首位数码（即 10^{k-1} 位上的数码），由归纳假设每组中所有数的各个数码之和为 $45(k-1)\times10^{k-2}$。共有十组，故包括首位数码在内，其数码总和为

$$45(k-1)10^{k-2}\times10+(1+2+\cdots+9)$$
$$\times10^{k-1}=45k10^{k-1}。$$

得证命题对一切自然数 n 成立。

2. (i) 不成立，(ii)、(iii)、(iv) 均成立。

3. 若 $a=b=c$，显然。注意到 $37\times3=111$，且 $111|\overline{aaa}$。当 a,b,c 不全相同时，就有 37 能整除

$$\overline{abc}-\overline{aaa}=(b-a)\times10+(c-a),$$

所以上式右边只能是 $37,-37,74$ 或 -74。于是

$$\overline{bca}-\overline{aaa}=(b-a)\times100+(c-a)\times10$$

只能是 $370,-370,740$ 或 -740，得 $37|\overline{bca}$；又同样

$$\overline{cab}-\overline{aaa}=(c-a)\times100+(b-a),$$

只能是 $703,-703,407$ 或 -407，得 $37|\overline{cab}$，证毕。

4. 因 $7\times11\times13=1001$，而 $\overline{abcabc}=\overline{abc}\times1001$。

5. 由 $9|\overline{4a77b}$，故 $4+a+7+7+b=9k'$，即 $a+b=9k$。又 $11|\overline{4a77b}$，所以 $4+7+b-a-7=11l$，即 $b-a=11l-4$。因此得 $b=\dfrac{1}{2}(9k+11l)-2$。由于 $0\leqslant a\ \ b\leqslant9$，所以只有 $k=l=1$ 满足。解得 $b=8$，$a=1$。即 41778 能被 99 整除。

6. 由于 $99|n$，所以 $9|n$，因此 $9|S_1(n)$，即 $S_1(n)=9k$。又 $11|n$，在 $n\neq0$ 时可证 $S_1(n)\neq9$，因若 $S_1(n)=9$，

$\tilde{S}_1(n)=11l \leqslant S_1(n)=9$，那么 $\tilde{S}_1(n)=0$。这样

$$S_1(n)+\tilde{S}_1(n)=2(a_0+a_1+\cdots)=9,$$

这是不可能的。因此得 $S_1(n)\geqslant 18$。

7. 因为

$$7|1001,\ 7|10101,\ 1979=3\times 659+2,$$

所以数

$$\underbrace{\underbrace{10101}\ \underbrace{10101}\cdots\underbrace{10101}}_{659\text{ 组}}\ \underbrace{00\cdots0}_{2^{1979}-2\times 660\text{ 个}}\ 1001$$

就是满足所说条件且能被 7 整除的整数。

8. 四位数 $\overline{abca}=(5c+1)^2$，即

$$1000a+100b+10c+a=(5c+1)^2$$

$$1000a+100b-25c^2=1-a$$

$25|(1-a)$，因此，$a=1$，代入得 $c^2=4(b+10)$，所以 c 为偶数，记 $c=2d$，代入得 $d^2=b+10$，所以只有 $b=6$，$d=4$，由此 $c=8$，所求四位数为 $41^2=1681$。

9. 记 $N=\overline{a_0a_1\cdots a_{n-1}}$，$0\leqslant a_i<10$ $(i=1,\cdots,n-1)$。故

$$N\geqslant a_0\times 10^{n-1}>a_0\times a_1\times\cdots\times a_{n-1}$$

这就证明了 n 位数 N，当 $n>1$ 时恒大于其数码之积。

10. 记此两位数为 $\overline{ab}$，由题设

$$10a+b=b^2+a \text{ 即 } 9a=b(b-1),$$

所以 $9|b$，得 $b=9$，$a=8$。所求两位数为 89。

11. 记这样的两位数为 $\overline{ab}$，由题设

$$10a+b=abk。$$

所以 $a|b$，$b|10a$。即有整数 q、q'，使 $10a=bq$，$b=aq'$。具体讨论可知：$a=1$，$b=1,2,5$；$a=2$，$b=4$；$a=3$，$b=6$。即这样的两位数有

$$11,12,15,24,36$$

等五个。

12. 记此数为 $\overline{ab\cdots cd}$，由题设

$$\overline{dc\cdots ba} = 4 \times \overline{ab\cdots cd}。$$

由于等式两边的两数其位数相同，所以 $0 \leqslant a \leqslant 2$。又由等式可知 a 为偶数且 $a \neq 0$，故得 $a = 2$。所以 $d = 8$，直接试算知它至少为一个四位数。此时 b、c 应满足

$$40b + 4c + 3 = 10c + b \text{ 即 } 13b + 1 = 2c，$$

所以 $b = 1$，$c = 7$。所求的数为 2178。

13. 由 bd 的十位数码等于 $a + c$，故 $1 \leqslant a + c \leqslant 9$。又

$$a + b + c + d = 26 \qquad (*)$$

所以 $17 \leqslant b + d \leqslant 25$。但 b、d 是两个数码，所以 $17 \leqslant b + d \leqslant 18$。

若 $b + d = 17$，则 $bd = 72$，由上知 $a + c = 7$，此时不满足(*)。

若 $b + d = 18$，则 $bd = 81$，得 $a + c = 8$。再由 $bd - c^2 = 2^n(n \neq 0)$，知 $c^2 = 81 - 2^n$，即 c^2 为奇数，因此 c 只能是 1、3、5、7。直接代入试算知 $c = 7$，故 $a = 1$。所求的数是 1979。

14. 注意到代数恒等式

$$a(a + p)(a + 2p)(a + 3p) = (a^2 + 3ap + p^2)^2 - p^4$$

在 $b(>5)$ 进位制中，让 $a = 1110 = b^3 + b^2 + b$，$p = 1$ 代入，那么 $a + p = 1111$，$a + 2p = 1112$，$a + 3p = 1113$，而

$$a^2 + 3ap + p^2 = b^6 + 2b^5 + 3b^4 + 5b^3 + 4b^2 + 3b + 1。$$

即得在 $b(>5)$ 进位制中成立着等式：

$$1110 \times 1111 \times 1112 \times 1113 = (1235431)^2 - 1。$$

15. 在基 $b(\geqslant 10)$ 的 b 进位表示中恒成立不等式

$$2 \times 297 < 2 \times 300 = 600 < 792 < 800 = 4 \times 200 < 4 \times 297。$$

所以若在 b 进位制中 792 能被 297 整除时其商 q 应等于 3，$792=3\times297$。即有

$$7b^2+9b+2=3\times(2b^2+9b+7)。$$

此即 $b^2-18b-19=0$，解得 $b=19$。即在 19 进位制中 792 能被 297 整除。

习题 10

1. 因为对任何正整数 n 有

$$(n^2+n)^2=n^4+2n^3+n^2<n^4+2n^3+2n^2+2n+1$$
$$<n^4+2n^3+3n^2+2n+1=(n^2+n+1)^2。$$

介于相继两平方数之间的数 $n^4+2n^3+2n^2+2n+1$ 不是平方数。

2. 四位数就是 1000 至 9999 间的整数，加上 400 后在 1400 至 10399 之间。这时有

$$38^2=1444>1400,$$
$$101^2=10201<10400,$$
$$102^2=10404>10399,$$

故共有 38，39，…，101 等 64 个。即有 64 个四位数，在加上 400 后分别为 $38^2,39^2,\cdots,101^2$。

3. 在 b 进位制中，$11111=b^4+b^3+b^2+b+1$，而

$$(b^2+b/2)^2<b^4+b^3+b^2+b+1$$
$$<\left(b^2+\frac{b}{2}+1\right)^2。$$

若不等式的中间项是一个完全平方数，那么应满足关系式

$$(b^2+(b+1)/2)^2=b^4+b^3+b^2+b+1$$

即 b 应满足 $b^2-2b-3=0$，解得 $b=3$，$b=-1$（不合）。在 $b=3$ 时 $11111=(102)^2$。

4. 由假设可知这个四位数

$$N^2=\overline{abcd}=\overline{(c+8)bc(b+4)}=\overline{cbcb}+8004$$
$$=\overline{cb}\times 101+7979+25$$
$$=(\overline{cb}+79)\times 101+25$$
即$(\overline{cb}+79)\times 101=(N-5)(N+5)$。由于 101 是素数，所以 $N-5=101$ 或 $N+5=101$，解得 $N=106$，96，代入验算知 106^2 不是四位数，故 $N=96$ 时 $N^2=9216$ 满足题设条件。

5. 设原数为 $\overline{ab}=10a+b$，倒排后为 $\overline{ba}=10b+a$。按题设

$$(10a+b)-(10b+a)=9(a-b)$$

是一个平方数，所以 $a-b$ 是一个完全平方数，因此 $a-b$ 可取 0,1,4,9 。

$a=b$ 时，有 11,22,…,99 等九个解；

$a-b=1$ 时，有 10,21,32,…,98 等九个解；

$a-b=4$ 时，有 40,51,…95 等六个解；

$a-b=9$ 时，仅有 90 一个解，总共有 25 个解。

6. 记此自然数为 n，按题意有

$$n+200=a^2,\ n+292=b^2。$$

故 $b^2-a^2=92$，即 $(b-a)(b+a)=92$。易知 $b-a$ 与 $b+a$ 同奇偶，此时 92 仅有 2×46，即同为偶数的积。所以得

$$b-a=2,\ b+a=46,$$

解得 $b=24, a=22$，代入求得 $n=284$ 。

7. 写 5 个相继正整数为 $n-2, n-1, n, n+1, n+2$。它们的平方和是 $5(n^2+2)$。若有平方和 $5(n^2+2)=a^2$ 即是完全平方数，那么 $5|a^2$，所以 $5|a$，因此 $5^2|a^2$，从而得 $5|(n^2+2)$。这样 n^2 的末位数码只可能为 8 或 3。但本节开始已指出整数 n 的平方的末位数只能为 0,1,4,5,6,9 不能为

8 或3，矛盾。故 $5(n^2+2)$ 不可能是平方数。

8. 若 $N=a^2$，其个位数码为 5，那么 a 的个位数码也为 5，所以N的最初二个数码为 25，且由 $a=b\times 10+5$，得

$$N=a^2=100b^2+100b+25=100b(b+1)+25$$

即N应为 $8k+1$ 型的数。但由题设 $N=5\cdots5525=8k'+5$，矛盾。

若 $N=a^2$，个位数码不为 5，那么十位数码必须为 5。由本节开始知，末两位只能是 56，同上讨论可知不是平方数。

9. 由题设知 $a+b=ab/c$。因 a、b 是整数，故 $c=qr$，使 $q|a$，$r|b$，由 $(a,b,c)=1$，所以 $(q,r)=1$。记 $a=mq$，$b=pr$。代入得

$$mq+pr=\frac{mq\cdot pr}{qr}=mp \qquad (*)$$

所以 $m|pr$。由于 $(a,b,c)=1$，所以 $(m,r)=1$，得 $m|p$。此外又有 $p|mq$，同理 $(p,q)=1$，所以 $p|m$，由此得 $p=m$。代入$(*)$式得 $p(q+r)=p^2$，即 $q+r=p$。从而得

$$a+b=pq+pr=p(q+r)=p^2,$$
$$a-c=pq-qr=q(p-r)=q^2,$$
$$b-c=pr-qr=r(p-q)=r^2。$$

10. 用反证法。若 $m(m+1)=a^l$，由于m与 $m+1$ 互素，由标准分解式可知m及 $m+1$ 都是某整数的 l 次方，而这显然是不可能的。因为如当 $m=b^l$ 时

$$m=b^l<m+1<(b+1)^l \quad (l>1)。$$

即 $m+1$ 不能是某整数的 l 次方。

习题 11

1. 由于

$$1^3+2^3+\cdots+n^3=\left[\frac{1}{2}n(n+1)\right]^2,$$

$$1^3+3^3+\cdots+(2n-1)^3=n^2(2n^2-1)。$$

所以

$$2^3+4^3+\cdots+(2n)^3=8\cdot\left[\frac{1}{2}n(n+1)\right]^2$$

$$=2n^2(n+1)^2。$$

按题意得

$$2n^2(n+1)^2-n^2(2n^2-1)=n^2(4n+3)$$

$$=2240=8^2\times 35,$$

解得 $n=8$。

2. 若不然，记此数列为 $p_1, p_2, \cdots, p_r, \cdots$，其公差 $d\neq 0$。显然，素数 $p_1>1$，$d\geqslant 1$。那么该等差数列的 p_1+1 项为

$$p_{1+p_1}=p_1+p_1d=p_1(1+d),$$

它不是素数，由此矛盾，得证命题成立。

3. 设 p、q 为任给的自然数，$p>q$，那么

$$a=p(p+q),\ b=2pq,\ c=q(p+q)$$

就满足所述要求。事实上，此时

$$ab=2p^2q(p+q),\ ac=pq(p+q)^2,\ bc=2pq^2(p+q)$$

之间的差

$$ab-ac=pq(p^2-q^2),\ ac-bc=pq(p^2-q^2)$$

相等，即 ab、ac、bc 成等差数列。（由此与 a、b、c 成比例的数也满足。）

4. 若 $(n, a+id)=1$ $(i=0, 1, \cdots, n-1)$，那么 $a+id$ 被 n 除的 n 个余数中没有一个为 0，所以必有 $a+id$ 与 $a+jd$ 的余数相同，由此 $n|[(a+id)-(a+jd)]$，即 $n|(i-j)d$。若 $(n,d)=1$，那么就有 $n|(i-j)$，这是不可

能的，因此 $(n,d)\neq 1$，即 $(n,d)>1$。

5．设相继 k 个自然数 $a,a+1,\cdots,a+(k-1)$ 之和为 1000，即有

$$1000=\frac{1}{2}[2a+(k-1)]k \text{ 即 } k(2a+k-1)=2^4 5^3。$$

此时 k 与 $2a+k-1$ 的奇偶性不同，因此有解：

$k=1$，$a=1000$；$k=5$，$a=198$；$k=25$，$a=28$；

$k=16$，$a=55$。

所求的自然数组为

$$1000;\quad 198,199,\cdots,202;$$
$$28,29,\cdots 52;\quad 55,56,\cdots,70$$

等四组。

6．仿照例 5 用数学归纳法证明之即得。

7．显然 $p_1\neq 2$，因此其公差 d 必为偶数。由题设 $6\nmid d$，那么必有 $3\nmid d$，(因不然当 $3|d$ 时就有 $6|d$)。由此三个素数 p_1，$p_2=p_1+d$，$p_3=p_1+2d$。我们来证 $p_1=3$。

若 $p_1=3l+1$，那么当 $d=3k+1$ 时，$p_3=3(2k+l+1)$ 不是素数，当 $d=3k+2$ 时，$p_2=3(k+l+1)$ 不是素数；

若 $p_1=3l+2$，那么当 $d=3k+1$ 时，$p_2=3(k+l+1)$ 不是素数，当 $d=3k+2$ 时，$p_3=3(2k+l+2)$ 不是素数。

由此即得必有 $p_1=3$。因此对于给定的 d，$6\nmid d$，至多只有一组素数 p_1，$p_2=p_1+d$，$p_3=p_1+2d$ 成等差数列。在 $d\leqslant 20$ 时有下列 6 组：

$d=2$：3，5，7；$d=4$：3，7，11；

$d=8$：3，11，19；$d=10$：3，13，23；

$d=14$：3，17，31；$d=20$：3，23，43。

8. 由数学归纳法易证

$$x_n = \frac{2^{n+1}+(-1)^n}{3},$$

$$y_n = 2\times 3^n + (-1)^{n-1} \quad (n=0,1,2\cdots)。 \qquad (1)$$

显然当 $n \geqslant 1$ 时 $x_n < y_n$。我们来证不存在正整数 m 和 n 使得 $x_m = y_n$。

用反证法。若不然有正整数 m、n 使 $x_m = y_n$，把它们的表示式代入，经整理后得

$$2^m - 3^{n+1} = \begin{cases} 2 & 当\ 2\nmid m,\ 2\nmid n\ 时, \\ -1 & 当\ 2\nmid m,\ 2\mid n\ 时, \\ 1 & 当\ 2\mid m,\ 2\nmid n\ 时, \\ -2 & 当\ 2\mid m,\ 2\mid n\ 时。\end{cases} \qquad (2)$$

现在分别来讨论。

当 $2\nmid n$，$2\nmid m$ 时，此时有 $2^m - 2 = 3^{n+1}$。此式左边为偶数，右边为奇数，所以无解。即不可能有 $x_m = y_n$。

当 $2\mid n$，$2\mid m$ 时，此时有 $2^m + 2 = 3^{n+1}$，同样无正整数解。(除去 $m=n=0$，此时确有 $x_0 = y_0 = 1$)。

当 $2\nmid m$，$2\mid n$ 时，由(2)得

$$2^m = 3^{n+1} - 1$$

$$= 2(3^n + 3^{n-1} + \cdots + 3 + 1) = 2\times(奇数)$$

此时仅当右边奇数为1时成立等式，即 $m=1$，$n=0$。这就是 $x_1 = y_0 = 1$。

当 $2\mid m$，$2\nmid n$ 时，由(2)得

$$2^m = 3^{n+1} + 1 = (4-1)^{n+1} + 1 = 4K + 2。$$

当 $m \geqslant 1$ 时，由 m 为偶数，左边是4的倍数，但 $4\nmid 4K+2$，矛盾。因此 $m<1$，即 $m=0$，此时左边为1，但右边 $3^{n+1}+1>1$，矛盾。即此时也不可能有 $x_m = y_n$。

综上所述，欲 $x_m = y_n$，仅当 $m=0,1$，$n=0$。除此

以外无正整数 m、n 使之成立。证毕。

9. 由例1已证此时等差数列的公差 d 必被 6 整除，仿照例 8 可证 $5|d$ 且 $7|d$。由于 5、6、7 两两互素，所以 $5\times6\times7|d$，即 $d=210k$。

按题意

$p_{10}=p_1+9d=p_1+9\times210k=p_1+1890k<3000$，

由此得 $0<k\leqslant1$，故 $k=1$。因此 $p_{10}=p_1+1890<3000$，即

$$p_1<3000-1890=1110。$$

现在我们只要求得 p_1，就有可能求得小于 3000 而成等差数列的十个素数。

为此，首先我们来证 $p_1=11$ 或 $11l+1$，即 p_1 为 11 或被 11 除的余数为 1。注意到 $210=11\times19+1$，因此

$$p_{m+1}=p_1+210m=11\times19m+(p_1+m)。$$

若 $p_1=11l+2$，那么 $p_{10}=11\times19\times9+(11l+2+9)=11(l+172)$ 就不是素数。同理，若 $p_1=11l+3$，则 $p_9=11(l+153)$ 不是素数，依此同理可得 p_1 被 11 除的余数不能是 $2,3,\cdots,10$。若 $p_1\neq11$，那么由 p_1 是素数，所以也不能是 11 的倍数，这就得证 $p_1=11$ 或 $11l+1$。

其次我们来证 p_1 被 13 除的余数只能是 2，4，6，8，10 或 12 之一。注意到 $210=13\times16+2$，

$p_{m+1}=p_1+(13\times16+2)m=13\times16m+(p_1+2m)$，

由于 p_{m+1} 为奇数，若 $p_1=13l+1$，那么 $p_7=13\times16\times6+(13l+13)=13(l+97)$ 不是素数。同理 p_1 被 13 除的余数不能是 3，5，7，9，11。又由 p_1 是素数，且被 11 除的余数只能为 1，所以 $p_1\neq13l$。这就得证 p_1 被 13 除的余数只能是 2，4，6，8，10 或 12 之一。

综合上述两者，除 p_1 可能为 11 外，$p_1=11l+1$。今记

$l=26r+s$ ($s=0,1,\cdots,25$)，代入得 $p_1=286r+11s+1$。此时由于 p_1 为奇数，故 $11s+1$ 只能取

$$1,23,45,67,89,111,133,155,177,199。$$

由 p_1 被 13 除的余数只能为 2，4，6，8，10 或 12 之一。所以 $11s+1$ 被 13 除的余数也只能是这六个数，因此 $11s+1$ 只能取 23,45,67,155,177,199 之一。又因 $p_1<1110$。故 p_1 的可能值为下列诸数之一：

$$11;23,309,585,881;45,331,615,903;$$

$$67,353,637,925;155,441,727,1013;$$

$$177,463,749,1035;199,485,771,1051。$$

而其中素数只有

$$11,23,881,331,67,353,727,1013,463,199。$$

我们已知 $d=210$。直接验证如当 $p_1=11$ 时，$p_2=221=13\times17$ 不是素数。通过验算，最后得仅当 $p_1=199$ 时，有满足题意的十个成等差数列的素数，它们是：

$$199,409,619,829,1039,1249,1459,1669,1879,2089。$$

习题 12

1. (i) $7^2=10\times4+9$，所以 $7^2\equiv9\equiv-1 \pmod{10}$。

$7^3=7^2\times7$，所以 $7^3\equiv63\equiv3 \pmod{10}$。

$7^4=(7^2)^2$，所以 $7^4\equiv(-1)^2\equiv1 \pmod{10}$。

(ii) $a\equiv-1 \pmod m$，由性质 25 得 $a^2\equiv(-1)^2\equiv1 \pmod m$。

$$a^{2k}\equiv(-1)^{2k}\equiv1 \pmod m,$$

$$a^{2k+1}\equiv(-1)^{2k+1}\equiv-1 \pmod m。$$

又由 $a\equiv-1 \pmod m$，所以也有 $a^{2k+1}\equiv a \pmod m$。

2. 因为

$$63!-61!=61!(63\times62-1)=61!\times5\times11\times71,$$

所以 $63! \equiv 61! \pmod{71}$。

3. (i) 记 $a = a_1 d$, $b = b_1 d$, $m = m_1 d$。
若 $a \equiv b \pmod{m}$，那么 $m \mid (a-b)$，即 $a - b = km$，代入得 $(a_1 - b_1)d = km_1 d$，即有 $a_1 - b_1 = km_1$，所以 $m_1 \mid (a_1 - b_1)$，因此 $a_1 \equiv b_1 \pmod{m_1}$。

(ii) 显然，一般是不成立的，如 $8 \equiv 3 \pmod{5}$，而 $64 \not\equiv 9 \pmod{25}$。一般地，当 $a \equiv b \pmod{m}$，若记 $(m, a+b) = d$，那么欲 $a^2 \equiv b^2 \pmod{m^2}$ 当且仅当

$$a \equiv b \left(\bmod \frac{m^2}{d}\right)。$$

证明从略。

4 (i) 因为

$$a_0 \equiv a_0 \pmod{11},\ a_2 \times 10^2 \equiv a_2 \pmod{11}, \cdots,$$
$$a_{2k} \times 10^{2k} \equiv a_{2k} \pmod{11}, \cdots$$
$$a_1 \times 10 \equiv -a_1 \pmod{11},\ a_3 \times 10^3 \equiv -a_3 \pmod{11}, \cdots,$$
$$a_{2k+1} \times 10^{2k+1} \equiv -a_{2k+1} \pmod{11},$$

所以

$$N = a_0 + a_1 \times 10 + \cdots + a_n \times 10^n$$
$$\equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$$
$$\equiv \sum_{i=0}^{n} (-1)^i a_i \pmod{11}。$$

(ii) 因为 $7 \times 11 \times 13 = 1001$。故同样有

$$C_0 \equiv C_0 \pmod{1001},\ C_1 \times 1000 \equiv -C_1 \pmod{1001}, \cdots$$

所以 $N = C_0 + C_1 \times 1000 + \cdots + C_n \times 1000^n$

$$\equiv (C_0 + C_2 + \cdots) - (C_1 + C_3 + \cdots)$$
$$\equiv \sum_{i=0}^{n} (-1)^i C_i \pmod{1001}。$$

5. 当 a 为偶数时，$a^2 \equiv 0$ 或 $4 \pmod{8}$；当 a 为奇数时，

$a^2\equiv1\pmod 8$。所以 $a^2+b^2+c^2\equiv x\pmod 8$，$x$ 的可能值有 0,1,2,3,4,5,6，但 $x\neq 7$。

6. 记 1979 年国庆节为 a，那么 $a\equiv1\pmod 7$。从 1979 至 2000 年共 21 年，其中平年每年 365 天，闰年每年 366 天。这段时间内恰为四年一闰，共有 1980，1984，…，2000 等 6 个闰年。所以从 1979 年国庆至 2000 年 10 月 1 日国庆共经天数是

$$365\times21+6\equiv6\pmod 7。$$

所以 2000 年 10 月 1 日是

$$a+365\times21+6\equiv1+6\equiv0\pmod 7,$$

这就是说恰为星期天。

7. 这就是要求证明 $1000\mid(n^{101}-n)$。由于 $(n,10)=1$，所以只要证明 $1000\mid(n^{100}-1)$，即 $n^{100}\equiv1\pmod{1000}$。

因 $(n,10)=1$，所以 n 为奇数且 $5\nmid n$。当 n 为奇数时

$$n^{100}-1=(n^{50}+1)(n^{25}+1)(n^{25}-1),$$

所以 $8\mid(n^{100}-1)$。又 $5\nmid n$，由例 5 知 $125\mid(n^{100}-1)$。由此可得 $1000\mid(n^{100}-1)$，即 $n^{100}\equiv1\pmod{1000}$。

8. 奇数 a 可以写成 $4k\pm1$ 型。

$$\begin{aligned}a^{2^n}&=(4k\pm1)^{2^n}\\&=(4k)^{2^n}\pm2^n(4k)^{2^n-1}+\cdots\pm2^n(4k)+1,\end{aligned}$$

所以得证

$$a^{2^n}\equiv1\pmod{2^{n+2}}。$$

习题 13

1. 由例 1 的证明过程可知，存在整数 n，m 使得

$$131\mid\overbrace{11\cdots1}^{n}\ \overbrace{0\cdots0}^{m}。$$

但

$$\overbrace{11\cdots1}^{n}\ \overbrace{0\cdots0}^{m}=\overbrace{11\cdots1}^{n}\times10^{m}。$$

由于$(131,10)=1$，所以$(131,10^m)=1$，因此$131|\overbrace{11\cdots1}^{n}$。

2. 这是第1题的一个推广，论证仿上题即得。

3. 由性质27(i)，只需证明 $a,2a,\cdots,ma$ 等m个整数对于模m互不同余就够了。用反证法，若不然有 $1\leqslant l<k\leqslant m$，使得 $ka\equiv la(\bmod m)$，那么由性质24，$ka-la\equiv0(\bmod m)$。由性质23知 $m|(k-l)a$。因为 $(m,a)=1$，所以 $m|(k-l)$，而这是不可能的，这就得证 $a,2a,\cdots,ma$ 对于模m是两两互不同余的。

4 同上题一样。若 $ka_i+l\equiv ka_j+l(\bmod m)$，由性质25(i)，那么 $ka_i\equiv ka_j(\bmod m)$。因$(k,m)=1$，所以由性质25(ii)得 $a_i\equiv a_j(\bmod m)$。这与 $a_1,a_2,\cdots,a_m$为模m的完全剩余组相矛盾。所以得证 $\{ka_i+l,i=1,2,\cdots,m\}$ 是模m的一个完全剩余组。

5. 仿照例3完全类似地可得。

6. 因为

$$7^2\equiv9\equiv-1(\bmod 10),\ 7^3\equiv-7\equiv3(\bmod 10),$$
$$7^4\equiv1(\bmod 10),$$

所以 $7^{4k+1}\equiv7(\bmod 10)$。又因

$$17\equiv1(\bmod 4),\ 17^{27}\equiv1^{27}\equiv1(\bmod 4),$$

即 $17^{27}=4k+1$。所以得

$$7^{17^{27}}=7^{4k+1}\equiv7(\bmod 10),$$

即 $7^{17^{27}}$ 的末位数码是7。

7. 因为

$$21\equiv10\equiv-1(\bmod 11),\ 21^2\equiv1(\bmod 11),$$

所以 $21^{2k+1}\equiv10(\bmod 11)$。又 21^{21} 显然是奇数，即有整数k使得 $21^{21}=2k+1$。所以得

$$21^{21^{21}} \equiv 21^{2k+1} \equiv 10 \pmod{11},$$

即 $21^{21^{21}}$ 被 11 除的余数为 10。

8. 因为

$$3^5 = 243 \equiv 43 \pmod{100},\quad 3^{10} \equiv 49 \pmod{100},$$

$$3^{20} \equiv 1 \pmod{100},$$

所以 $3^{20k} \equiv 1 \pmod{100}$。而 $999 = 20 \times 49 + 19$，

所以 $3^{999} = (3^{20})^{49} \times 3^{19} \equiv 3^{19} \pmod{100}$。

直接计算可得 $3^{19} \equiv 67 \pmod{100}$，即有 $3^{999} \equiv 67 \pmod{100}$，这就是说 3^{999} 的末两位数码是 67。

$$21^{21^{21}} \equiv 21^{2k+1} \equiv 10 \pmod{11},$$

即 $21^{21^{21}}$ 被 11 除的余数为 10。

8. 因为

$$3^5 = 243 \equiv 43 \pmod{100}, \quad 3^{10} \equiv 49 \pmod{100},$$

$$3^{20} \equiv 1 \pmod{100},$$

所以 $3^{20k} \equiv 1 \pmod{100}$。而 $999 = 20 \times 49 + 19$，

所以 $3^{999} = (3^{20})^{49} \times 3^{19} \equiv 3^{19} \pmod{100}$。

直接计算可得 $3^{19} \equiv 67 \pmod{100}$，即有 $3^{999} \equiv 67 \pmod{100}$，

这就是说 3^{999} 的末两位数码是 67。